

ESSENTIAL RECIPES FOR SUCCESS WITH YOUR FORTIGATE



NOW WITH MORE RECIPES  
**EXPANDED**  
VERSION

# THE FORTIGATE WORLD'S MOST POWERFUL NETWORK SECURITY COOKBOOK

**FORTINET**

The FortiGate Cookbook 5.0.7 (Expanded Version)  
Essential Recipes for Success with your FortiGate

April 23, 2014

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Knowledge Base - <http://kb.fortinet.com>

Technical Documentation - <http://docs.fortinet.com>

Video Tutorials - <http://video.fortinet.com>

Training Services - <http://campus.training.fortinet.com>

Technical Support - <https://support.fortinet.com>

Please report errors or omissions in this or any Fortinet technical document to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).



# Contents

- Change log..... 1**
- Introduction ..... 2**
- Tips for using the FortiGate Cookbook..... 3**
- Installing & Setup ..... 5**
  - Connecting a private network to the Internet using NAT/Route mode ..... 7
  - Extra help: NAT/Route mode..... 11
  - Quickly connecting a network to the Internet using DHCP..... 14
  - Extra help: Private networks with DHCP..... 16
  - Adding a FortiGate unit without changing the network configuration..... 18
  - Extra help: Transparent mode ..... 22
  - Using VDOMs to host two FortiOS instances on a single FortiGate unit..... 26
  - Verifying and updating the FortiGate unit’s firmware ..... 33
  - Setting up FortiGuard services..... 36
  - Extra help: FortiGuard ..... 38
  - Logging network traffic to gather information..... 39
  - Extra help: Logging ..... 43
  - Using FortiCloud to record log messages..... 44
  - Setting up a limited access administrator account..... 48
  - Using SNMP to monitor the FortiGate unit ..... 52
  - Setting up an explicit proxy for users on a private network..... 58
  - Adding packet capture to help troubleshooting..... 62

Protecting a web server on the DMZ network.....	65
Using port pairing to simplify transparent mode.....	69
Using two ISPs for redundant Internet connections .....	74
Adding a backup FortiGate unit to improve reliability .....	79
Associating a domain name with an interface that has a dynamic IP .....	84
Allowing VoIP calls using FortiVoice and FortiCall .....	86
Allowing access from the Internet to a FortiCamera unit .....	93
<b>Security Policies &amp; Firewall Objects .....</b>	<b>99</b>
Ordering security policies to allow different access levels.....	100
Using port forwarding on a FortiGate unit.....	104
Using AirPlay with iOS, AppleTV, FortiAP, and a FortiGate unit .....	109
Using AirPrint with iOS and OS X and a FortiGate unit.....	117
<b>Security Features .....</b>	<b>126</b>
Monitoring your network using client reputation.....	127
Controlling network access using application control .....	130
Using a custom signature to block web traffic from Windows XP .....	136
Protecting a web server from external attacks.....	141
Blocking outgoing traffic containing sensitive data.....	145
Preventing credit card numbers from escaping your network .....	150
Blocking access to specific websites .....	160
Extra help: Web filtering .....	163
Blocking HTTP and HTTPS traffic with web filtering.....	164
Limiting access to personal interest websites using quotas.....	169

Setting up YouTube for Education.....	173
Using web filter overrides to control website access.....	179
Inspecting traffic content using flow-based inspection .....	187
Analyzing your network traffic using a one-armed sniffer .....	192
Excluding specific users from security scanning .....	203
<b>Wireless Networking.....</b>	<b>207</b>
Setting up a temporary guest WiFi user.....	208
Setting up a network using a FortiGate unit and a FortiAP unit.....	215
Providing remote users access to the corporate network and Internet.....	220
Assigning wireless users to different networks using dynamic VLANs.....	226
Extending the range of a wireless network by using mesh topology.....	236
<b>IPv6.....</b>	<b>251</b>
Creating an IPv6 interface using SLAAC.....	252
<b>Authentication .....</b>	<b>256</b>
Identifying network users and applying web filters based on identity .....	257
Controlling when specific types of devices can access the Internet .....	263
Providing Single Sign-On for a Windows AD network with a FortiGate.....	267
Providing Single Sign-On in advanced mode for a Windows AD network.....	273
Providing Single Sign-On for Windows AD with LDAP .....	276
Allowing Single Sign-On access with a FortiGate and a FortiAuthenticator .....	280
Fortinet Single Sign-On in Polling Mode for a Windows AD network .....	284
Preventing security certificate warnings when using SSL inspection.....	290
Extra help: Certificates .....	294

Adding FortiToken two-factor authentication to a user account.....	295
Using two-factor authentication with IPsec VPN .....	299
Using two-factor authentication with SSL VPN .....	306
Authenticating SSL VPN users using LDAP .....	312
<b>SSL and IPsec VPN .....</b>	<b>320</b>
Providing remote users with access using SSL VPN .....	321
Connecting an Android to a FortiGate with SSL VPN .....	329
Configuring SSL VPN with strong authentication using certificates .....	337
Using IPsec VPN to provide communication between offices.....	344
Extra help: IPsec VPN .....	352
Using policy-based IPsec VPN for communication between offices.....	354
Providing secure remote access to a network for an iOS device .....	361
Connecting an Android to a FortiGate with IPsec VPN.....	369
Configuring a FortiGate unit as an L2TP/IPsec server .....	378
Configuring IPsec VPN with a FortiGate and a Cisco ASA .....	386
Creating a VPN with overlapping subnets.....	392
Using redundant OSPF routing over IPsec VPN .....	398

# Change log

Date	Change Description
April 23, 2014	<p>Added new section: IPv6</p> <p>New recipes:</p> <ul style="list-style-type: none"><li>- Analyzing your traffic using a one-armed sniffer</li><li>- Creating an IPv6 interface using SLAAC</li><li>- Fortinet Single Sign-On in Polling Mode for a Windows AD network</li></ul> <p>Removed recipe:</p> <ul style="list-style-type: none"><li>- Blocking large files from entering the network</li></ul> <p>Updated to FortiOS version 5.0.7</p>
March 5, 2014	<p>New recipes:</p> <ul style="list-style-type: none"><li>- Using a custom signature to block web traffic from Windows XP</li><li>- Preventing credit card numbers from escaping your network</li></ul> <p>Updated recipes:</p> <ul style="list-style-type: none"><li>- Connecting a private network to the Internet using NAT/Route mode</li><li>- Using IPsec VPN to provide communications between offices</li></ul>
February 3, 2014	<p>New recipes:</p> <ul style="list-style-type: none"><li>- Extra help: IPsec VPN</li></ul> <p>Reordered SSL and IPsec VPN section. Added FortiGate ports section to Tips for the FortiGate Cookbook. Added a note to Providing secure remote access to a network for an iOS device.</p> <p>Updated to FortiOS version 5.0.6</p>



# Introduction

The FortiGate Cookbook (Expanded Version) is a web-only version of the FortiGate Cookbook that will be continuously updated with new examples not contained in the print version. See the [Change log](#) for a list of the most recent additions.

The FortiGate Cookbook provides examples, or recipes, of basic and advanced FortiGate configurations to administrators who are unfamiliar with the unit. All examples require access to the graphical user interface (GUI), also known as the web-based manager.

Each example begins with a description of the desired configuration, followed by step-by-step instructions. Some topics include extra help sections, containing tips for dealing with some common challenges of using a FortiGate unit.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

The Cookbook is divided into the following chapters:

[Installing & Setup](#) explains the configuration of common network functions and the different network roles a FortiGate unit can have.

[Security Policies & Firewall Objects](#) describes security policies and firewall objects, which determine whether to allow or block traffic.

[Security Features](#) describes the core security features that you can apply to the traffic accepted by your FortiGate unit.

[Wireless Networking](#) explains how to configure and maintain a wireless network.

[IPv6](#) shows how to use the new IPv6 protocol with your FortiGate.

[Authentication](#) describes the FortiGate authentication process for network users and devices.

[SSL and IPsec VPN](#) explains the configuration and application of SSL and IPsec virtual private networks (VPNs).

This edition of the FortiGate Cookbook (Expanded Version) was written using FortiOS 5.0.7.

# Tips for using the FortiGate Cookbook

Before you get started, here are a few tips about using the FortiGate Cookbook:

## Understanding the basics

While the FortiGate Cookbook was written with new FortiGate users in mind, some basic steps, such as logging into the FortiGate unit, are not included in most recipes. This information can be found in the first example, “[Connecting a private network to the Internet using NAT/Route mode](#)” on page 7, or in the QuickStart guide for your FortiGate unit.

## Screenshots vs. text

The FortiGate Cookbook uses both screenshots and text to explain the steps of each example. The screenshots display the entire configuration, while the text highlights key details (i.e. the settings that are strictly necessary for the configuration) and provides additional information. To get the most out of the FortiGate Cookbook, start with the screenshots and then read the text for more details.

## Model and firmware

GUI menus, options, and interface names may vary depending on the FortiGate model you are using and the firmware build. For example, the menu **Router > Static > Static Routes** is not available on some models. Also, on different models, the Ethernet interface that would normally connect to the Internet could be named **port1**, **wan1**, **wan2**, or **external**.

Also, some features are only available through the CLI on certain FortiGate models, generally the desktop models (FortiGate/WiFi-20 to 90 Series).

## FortiGate ports

The specific ports being used in the documentation are chosen as examples. When you are configuring your FortiGate unit, you can substitute your own ports, provided that they have the same function.

For example, in most recipes, **wan1** is the port used to provide the FortiGate unit with access to the Internet. If your FortiGate uses a different port for this function, you should use that port in the parts of the configuration that the recipe uses **wan1**.

## IP addresses

IP addresses are sometimes shown in diagrams to make it easier to see the source of the addresses used in the recipe. When you are configuring your FortiGate unit, substitute your own addresses.

## Turning on features

Some FortiOS features can be turned off, which means they will not appear in the GUI. If an option required for a recipe does not appear, go to **System > Config > Features** and make sure that option has not been disabled.

## Text elements

**Bold** text indicates the name of a GUI field or feature. When required, *italic* text indicates information that you must enter.

## Selecting OK/Apply

Always select **OK** or **Apply** when you complete a GUI step. Because this must be done frequently, it is an assumed step and is not included in most recipes.

# Installing & Setup

The FortiGate unit provides protection for a variety of different network functions and configurations. This section contains information about the basic setup for common network functions as well as different roles that a FortiGate unit can have within your network.

This section contains the following examples:

- Connecting a private network to the Internet using NAT/Route mode
- Extra help: NAT/Route mode
- Quickly connecting a network to the Internet using DHCP
- Extra help: Private networks with DHCP
- Adding a FortiGate unit without changing the network configuration
- Extra help: Transparent mode
- Using VDOMs to host two FortiOS instances on a single FortiGate unit
- Verifying and updating the FortiGate unit's firmware
- Setting up FortiGuard services
- Extra help: FortiGuard
- Logging network traffic to gather information
- Extra help: Logging
- Using FortiCloud to record log messages
- Setting up a limited access administrator account
- Using SNMP to monitor the FortiGate unit
- Setting up an explicit proxy for users on a private network
- Adding packet capture to help troubleshooting

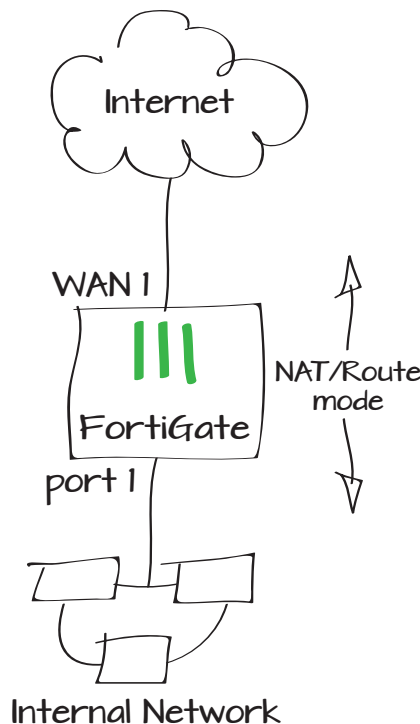
- Protecting a web server on the DMZ network
- Using port pairing to simplify transparent mode
- Using two ISPs for redundant Internet connections
- Adding a backup FortiGate unit to improve reliability
- Associating a domain name with an interface that has a dynamic IP
- Allowing VoIP calls using FortiVoice and FortiCall
- Allowing access from the Internet to a FortiCamera unit



# Connecting a private network to the Internet using NAT/Route mode

In this example, you will learn how to connect and configure a new FortiGate unit to securely connect a private network to the Internet. Typically, a FortiGate unit is installed as a gateway or router between a private network and the Internet, where the FortiGate operates in NAT/Route mode in order to hide the addresses of the private network from prying eyes, while still allowing anyone on the private network to freely connect to the Internet.

1. Connecting the network
2. Configuring the FortiGate unit's interfaces
3. Creating a policy to enable NAT/Route mode
4. Results



## Connecting the network

Connect the FortiGate WAN1 interface to your ISP-supplied equipment.

Connect the internal network to the FortiGate internal interface (typically port 1).

Power on the ISP's equipment, the FortiGate unit, and the PCs on the Internal network.

## Configuring the FortiGate unit's interfaces

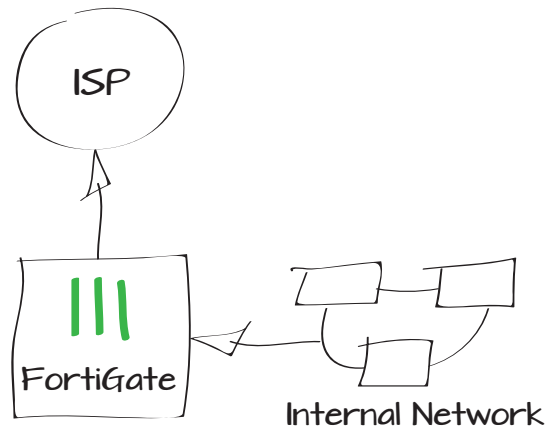
From a PC on the Internal network, connect to the FortiGate web-based manager using either FortiExplorer or an Internet browser.

You can configure the PC to get its IP address using DHCP and then browse to <https://192.168.1.99>. You could also give the PC a static IP address on the `192.168.1.0/255.255.255.0` subnet.

Login using **admin** and no password.

Go to **System > Network > Interface** and **Edit** the **wan1** interface.

Set the **Addressing Mode** to *Manual* and the **IP/Netmask** to your public IP.



Name	<input type="text" value="admin"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP/FortiSwitch
IP/Network Mask	<input type="text" value="172.20.120.14/255.255.255.0"/>
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access

Edit the **internal** interface.

Set the **Addressing Mode** to *Manual* and set the **IP/Netmask** the private IP of the FortiGate unit.

Go to **Router > Static > Static Routes** and select **Create New** to add a default route.

Set the **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set the **Device** to *wan1*, and set the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.



A default route always has a **Destination IP/Mask** of *0.0.0.0/0.0.0.0*. Normally, you would have only one default route. If the static route list already contains a default route, you can edit it or delete it and add a new one.

The FortiGate unit's **DNS Settings** are set to **Use FortiGuard Services** by default, which is sufficient for most networks. However, if you require the DNS servers to be changed, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE
IP/Network Mask	<input type="text" value="192.168.1.99/255.255.255.0"/>
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access
Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan1"/>
Gateway	<input type="text" value="172.20.120.2"/>
Distance	<input type="text" value="10"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)

**DNS Settings**

☐ Use FortiGuard Servers ☒ Specify

Primary DNS Server

Secondary DNS Server

Local Domain Name

# Creating a policy to enable NAT/Route mode

Go to **Policy > Policy > Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet.

Select **Enable NAT** and **Use Destination Interface Address** and click **OK**.



Some FortiGate models include this security policy in the default configuration. If you have one of these models, this step has already been done for you and as soon as your FortiGate unit is connected and the computers on your internal network are configured, they should be able to access the Internet.

## Results

On the PC that you used to connect to the FortiGate internal interface, open a web browser and browse to any Internet website. You should also be able to connect to the Internet using FTP or any other protocol or connection method.

Go to **Policy > Monitor > Policy Monitor** to view information about the sessions being processed by the FortiGate unit.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

☒ Firewall

☐ VPN

☒ Address

☐ User Identity

☐ Device Identity

port1

+

all

+

wan1

+

all

+

always

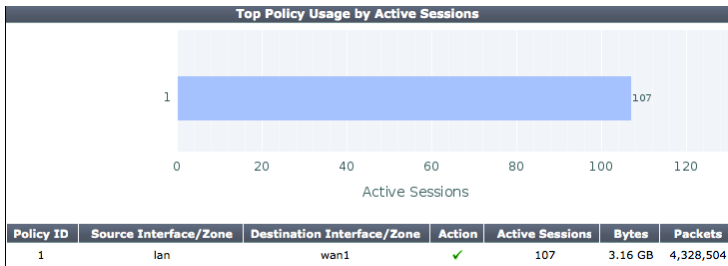
▼

ALL

+

ACCEPT

▼



# Extra help: NAT/Route mode

This section provides instructions for troubleshooting connection issues in situations when a NAT/Route configuration is used.

## 1. Use FortiExplorer if you can't connect to the FortiGate GUI or CLI

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

## 2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network and about the information provided by the FortiGate unit LED indicators.

## 3. Check the physical network connections.

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged. Also check the Unit Operation dashboard widget, which shows the connection status of FortiGate network interfaces (**System > Dashboard > Status**).

## 4. Verify that you can connect to the internal IP address of the FortiGate unit.

Use a web browser to connect to the web-based manager from the FortiGate internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`. If you cannot connect to the internal interface, verify the IP configuration of the PC. Go to the next step when you can connect to the internal interface.

## 5. Check the FortiGate interface configurations.

Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure it includes the proper addressing mode.

## 6. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the `execute ping` command to ping an address or domain name on the Internet. You can also use the `execute traceroute` command to troubleshoot connectivity to the Internet.



## 7. Verify the DNS configurations of the FortiGate unit and the PCs.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example:

```
ping www.fortinet.com
ping: cannot resolve www.fre.com: Unknown host
```

If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm the DNS server IP addresses are present and correct.

## 8. Verify the security policy configuration.

Go to **Policy > Policy > Policy** and verify that an internal -> wan1 security policy has been added and check the **Session** column to ensure that traffic has been processed. Check the configuration of the policy to make sure that **Enable NAT** and **Use Destination Interface Address** is selected.

## 9. Verify the static routing configuration.

Go to **Router > Static > Static Routes** and verify that the default route is correct. Go to **Router > Monitor > Router Monitor** and verify that the default route appears in the list as a static route. Along with the default route, you should see at least two connected routes, one for each connected FortiGate interface.



On some FortiGate models, routing options are configured by going to **System > Network > Routing** or through the CLI.

## 10. Disable web filtering.

A web filtering security policy may block access to the website that you are attempting to connect to. This could happen because the configuration of the default web filter profile is blocking access to the site.

It is also possible that FortiGuard Web Filtering has produced a rating error for the website, causing the web filter profile to block access. A rating error could occur for a number of reasons, including not being able to access FortiGuard. To fix this problem, go to **Security Profiles > Web Filter > Profile** and, in the default profile, enable **Allow Websites When a Rating Error Occurs**.

### 11. Verify that you can connect to the wan1 IP address of the FortiGate unit.

Once you have established that the internal network is operating, ping the FortiGate wan1 interface IP address. If you cannot connect to the wan1 interface, the FortiGate unit is not allowing internal to wan1 sessions.

### 12. Verify that you can connect to the gateway provided by your ISP.

Try pinging the default gateway IP address from a PC on the internal network.

### 13. Consider changing the MAC address of your external interface

Some ISPs do not want the MAC address of the device connecting to their network cable to change. If you have added a FortiGate unit to your network, you may have to change the MAC address of the external interface (typically, WAN1) by using the following CLI command:

```
config system interface
    edit wan1
        set macaddr <xx:xx:xx:xx:xx:xx>
    end
end
```

### 14. Reset the FortiGate unit to factory defaults and try again

If all else fails, use the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

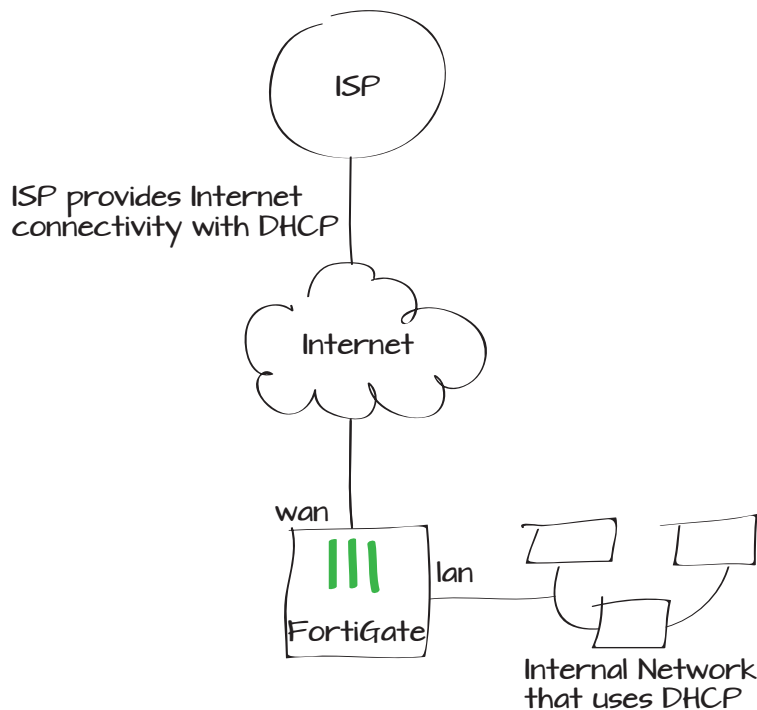
# Quickly connecting a network to the Internet using DHCP

In this example, you will learn how to use a FortiGate unit to securely connect to the Internet with minimal configuration, using DHCP.

## Requirements

- An ISP that provides connectivity with DHCP and accepts DHCP requests without authentication.
- A FortiGate default configuration that includes a DHCP server for the internal interface and a security policy that allows all sessions from the internal network to the internet.

1. Connecting to the ISP and to the internal network
2. Configuring your PCs
3. Results

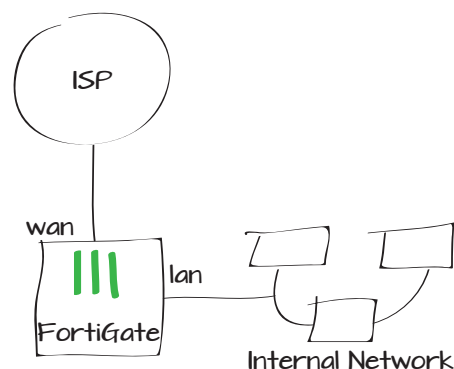


# Connecting to the ISP and to the internal network

Connect the FortiGate wan interface to your ISP-supplied equipment.

Connect the internal network to the FortiGate internal interface (in this example, lan).

Turn on the ISP's equipment, the FortiGate unit, and the PCs on the internal network.



# Configuring your PCs

If required, configure the PCs on the internal network to automatically get their network configuration using DHCP.



Each PC gets an address on the 192.168.1.0/255.255.255.0 subnet.

# Results

From any PC on the internal network, open a web browser and browse to any website. You should successfully connect to the Internet.

Go to **Policy > Policy > Policy** and select **Global View**. View **Sessions** and **Count** columns for information about the sessions being processed by the FortiGate.

If these columns are not visible, right-click on the menu bar, select **Sessions** and **Count**, and select **Apply**.

Status: **Connected**  
Ethernet is currently active and has the IP address 192.168.1.110.

Configure IPv4: Using DHCP

IP Address: 192.168.1.110

Subnet Mask: 255.255.255.0

Router: 192.168.1.99


Create New Edit Delete Section View Global View Search					
Seq.#	From	To	Action	Sessions	Count
1	lan	wan	✓ Accept	14	1,852,560 Packets / :
2	any	any	⊘ Deny		

# Extra help: Private networks with DHCP

This section provides instructions for troubleshooting connection issues when your network uses DHCP to connect to your ISP and configure your internal network.

## 1. Check the wan interface.

Verify that the wan interface is getting network settings from the ISP. Go to **System > Network > Interfaces**. Highlight the wan interface and select **Edit**. Confirm that the **Addressing Mode** is set to DHCP and that the **Distance** is set to 5, and ensure that **Retrieve default gateway from server** and **Override internal DNS** are both enabled.

Addressing mode	<input type="radio"/> Manual <input checked="" type="radio"/> DHCP <input type="radio"/> PPPoE
Status	connected 
Obtained IP/Netmask	172.20.120.229 255.255.255.0 <button>Renew</button>
Expiry Date	December 09, 2013 03:32 PM
Acquired DNS	8.8.8.8 None
Default Gateway	172.20.120.2
Distance	<input type="text" value="5"/>
Retrieve default gateway from server.	<input checked="" type="checkbox"/>
Override internal DNS.	<input checked="" type="checkbox"/>

If the IP address seems incorrect or missing, select **Renew** to renew the lease and get a new IP configuration from your ISP. If you cannot get a valid IP address this way, the FortiGate unit cannot communicate with the ISP's DHCP server.

## 2. Verify that your ISP automatically provides a DNS server with DHCP.

If your ISP does not supply a DNS server with DHCP, you can go to **System > Network > DNS** and manually add one.

## 3. Verify that your ISP supplies a default gateway with DHCP.

If your ISP does not supply a default gateway with DHCP, you can go to **Router > Static > Static Route > Create New** and manually add a default route that points from the wan interface to the ISP's default gateway.



#### 4. Check the internal network configuration.

If the internal network is configured to get IP addresses from the FortiGate DHCP server, go to **System > Interfaces**. In the **Address Range** highlight your interface and click **Edit**. Confirm that the DHCP server configuration uses system DNS settings as shown below.

DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<div><div><div>Create New</div><div>Edit</div><div>Delete</div></div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>192.168.1.110</td><td>192.168.1.210</td></tr></tbody></table></div>	Starting IP	End IP	192.168.1.110	192.168.1.210
Starting IP	End IP				
192.168.1.110	192.168.1.210				
Netmask	<input type="text" value="255.255.255.0"/>				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify				

#### 5. Confirm that your PC successfully receives its address using DHCP.

Go to **System > Monitor > DHCP Monitor** to view information about the PCs configured by the FortiGate unit DHCP server. There should be one entry here for each PC on the network that successfully receives its address using DHCP. The following example can be used for comparison.

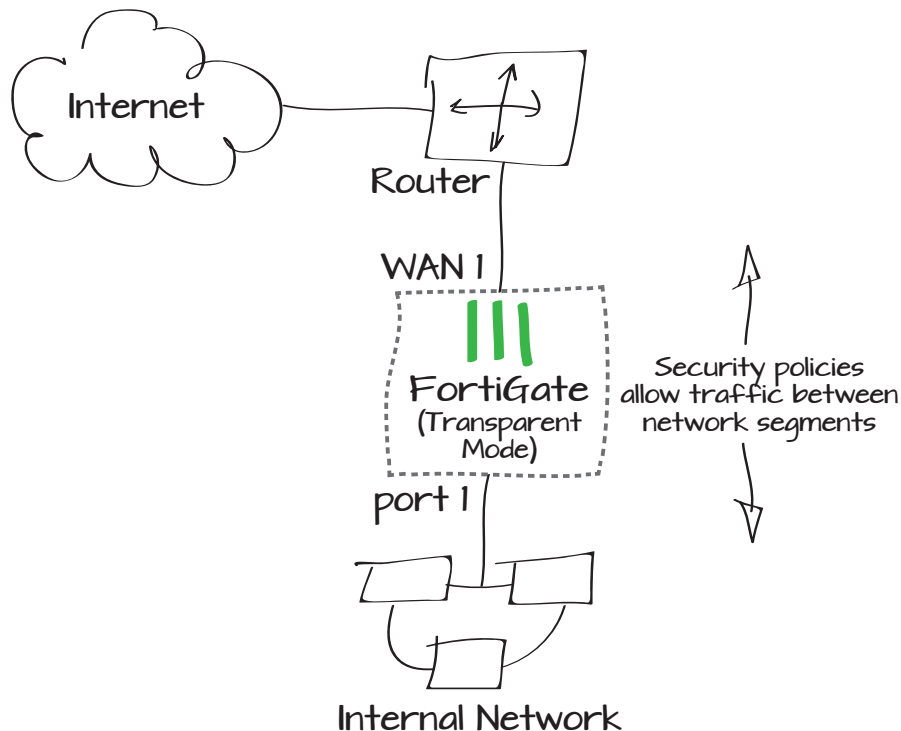
Interface	IP	MAC	Host Information	Expire	Status
lan	192.168.1.110	c4:2c:03:0b:0c:0f	Hostname: techdocs-Mini	Wed Dec 25 06:08:33 2013	Leased out

If problems persist, see [“Connecting a private network to the Internet using NAT/Route mode” on page 7](#).

# Adding a FortiGate unit without changing the network configuration

This section describes how to connect and configure a new FortiGate unit to protect a private network without changing the network configuration. This is known as Transparent mode and it allows you to add network security without replacing the router. The FortiGate unit blocks access from the Internet to the private network but allows users on the private network to connect to the Internet. The FortiGate unit monitors application usage and detects and eliminates viruses.

1. Connecting the FortiGate and configuring Transparent mode
2. Creating a security policy
3. Connecting the network
4. Results



# Connecting the FortiGate and configuring Transparent mode



Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Mode configuration, backup the configuration using the System Information dashboard widget.

Go to **System > Dashboard > Status > System Information** and beside **Operation Mode** select **Change**.

Set the **Operation Mode** to **Transparent**.

Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit the internal network.

You can now access the web-based manager by browsing to the Management IP (in the example, you would browse to *https://10.31.101.40*).

The FortiGate unit's **DNS Settings** are set to **Use FortiGuard Services** by default, which is sufficient for most networks. However, if you require the DNS servers to be changed, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

System Information	
Host Name	FG100D3G12801345 [Change]
Serial Number	FG100D3G12801345
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Mon Aug 26 10:24:54 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0228 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	17 day(s) 4 hour(s) 58 min(s)
Virtual Domain	Disabled [Enable]

Operation Mode	Transparent
Management IP/Netmask	10.31.101.40/255.255.255.0
Default Gateway	10.31.101.100

DNS Settings	
<input type="radio"/> Use FortiGuard Servers <input checked="" type="radio"/> Specify	
Primary DNS Server	208.91.112.53
Secondary DNS Server	208.91.112.52
Local Domain Name	

## Creating a security policy

Go to **Policy > Policy > Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet.

Under **Security Profiles**, enable **Antivirus** and enable **Application Control**.

Press **OK** to save the security policy








Power off the FortiGate unit.

## Connecting the network



Connect the FortiGate unit between the internal network and the router.

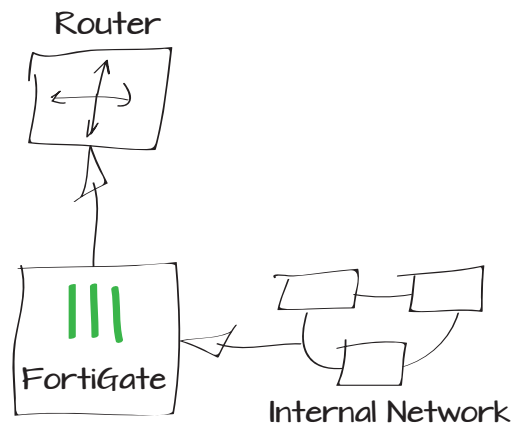
Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.

Power on the FortiGate unit.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	port1 
Source Address	all 
Outgoing Interface	wan1 
Destination Address	all 
Schedule	always 
Service	ALL 
Action	ACCEPT 

<b>Security Profiles</b>	
<input checked="" type="checkbox"/> Antivirus	default 
<input type="checkbox"/> Web Filter	default
<input checked="" type="checkbox"/> Application Control	default 



# Results

On the PC that you used to connect to the FortiGate internal interface, open a web browser and browse to any Internet website. You should also be able to connect to the Internet using FTP or any other protocol or connection method.

Go to **Policy > Monitor > Session Monitor** to view the sessions being processed by the FortiGate unit.



If a FortiGate unit operating in Transparent mode is installed between a DHCP server and PCs that get their address by DHCP, you must add a security policy to allow the DHCP server's response to get back through the FortiGate unit from the DHCP server to the DHCP client. The internal to wan1 policy allows the DHCP request to get from the client to the server, but the response from the server is a new session, not a typical response to the originating request, so the FortiGate unit will not accept this new session unless you add a wan1 to the internal policy with the service set to DHCP.

Protocol	Src Address	Src Port	Src NAT IP	Src NAT Port	Dst Address	Dst Port
tcp	10.31.101.50	4218			23.1.111.139	80
tcp	10.31.101.50	4224			63.84.95.34	80
tcp	10.31.101.50	4225			63.84.95.34	80
tcp	10.31.101.50	4220			63.84.95.34	80
tcp	10.31.101.50	4221			63.84.95.34	80
tcp	10.31.101.50	4222			63.84.95.34	80
tcp	10.31.101.50	4223			63.84.95.34	80
udp	10.31.101.50	1132			8.8.8.8	53
udp	10.31.101.50	2815			8.8.8.8	53

1 / 2

Total: 57

## Extra help: Transparent mode

This section provides instructions for troubleshooting connection issues when using a FortiGate in Transparent mode.

### 1. Use FortiExplorer if you can't connect to the FortiGate GUI or CLI

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

### 2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network and about the information provided by the FortiGate unit LED indicators.

### 3. Check the physical network connections.

Check the cables used for all physical connections between the PC, the FortiGate unit, and your ISP-supplied equipment to ensure that they are fully connected and do not appear damaged. Also check the Unit Operation dashboard widget, which indicates the connection status of FortiGate network interfaces (**System > Dashboard > Status**).

### 4. Verify that you can connect to the management IP address of the FortiGate unit from the Internal network.

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

### 5. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the `execute ping` command to ping an address or domain name on the Internet. You can also use the `execute traceroute` command to troubleshoot connectivity to the Internet.

## 6. Verify the DNS configurations of the FortiGate unit and the PCs on the internal network.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example:

```
ping www.fortinet.com
ping: cannot resolve www.fre.com: Unknown host
```

If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm the DNS server IP addresses are present and correct.

## 7. Verify the security policy configuration.

Go to **Policy > Policy > Policy** and verify that an internal -> wan1 security policy has been added and check the **Session** column to ensure that traffic has been processed.

## 8. Verify the static routing configuration.

Go to **System > Network > Routing Table** and verify that the default route is correct.

## 9. Disable web filtering.

A web filtering security policy may block access to the website that you are attempting to connect to. This could happen because the configuration of the default web filter profile is blocking access to the site.

It is also possible that FortiGuard Web Filtering has produced a rating error for the website, causing the web filter profile to block access. A rating error could occur for a number of reasons, including not being able to access FortiGuard. To fix this problem, go to **Security Profiles > Web Filter > Profile** and, in the default profile, enable **Allow Websites When a Rating Error Occurs**.

## 10. Verify that you can connect to the gateway provided by your ISP.

Try pinging the default gateway IP address from a PC on the internal network.

## 11. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, you should confirm that it can reach the FortiGuard network. The FortiGate unit must be able to connect to the network from its management IP address. If the following tests provide

incorrect results, the FortiGate unit cannot connect to the Internet from its management IP address. Check the FortiGate unit's default route to make sure it is correct. Check your Internet firewall to make sure it allows connections from the FortiGate management IP address to the Internet.

First, check the **License Information** dashboard widget to make sure the status of all FortiGuard services matches the services that you have purchased. The FortiGate unit connects to the FortiGuard network to obtain this information.

Go to **System > Config > FortiGuard**. Open web filtering and email options and select **Test Availability**. After a minute, the GUI should indicate a successful connection.

## 12. Check the FortiGate bridge table.

The bridge table is a list of MAC addresses of devices on the same network as the FortiGate unit and the FortiGate interfaces from which each MAC address was found. The FortiGate unit uses this table to determine where to forward a packet. If a the MAC address of a specific device is getting added to the bridge table, then packets to that MAC address will be blocked. This may appear as traffic going to a MAC address but no reply traffic coming back. In this situation, check the bridge table to ensure the correct MAC addresses have been added to the bridge table. Use the following CLI command to check the bridge table:.

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 wan1 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. This could indicate that the device is not connected or not operating. Check the device's network connections and make sure it is operating correctly.



### 13. Reset the FortiGate unit to factory defaults and try again

If all else fails, use the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

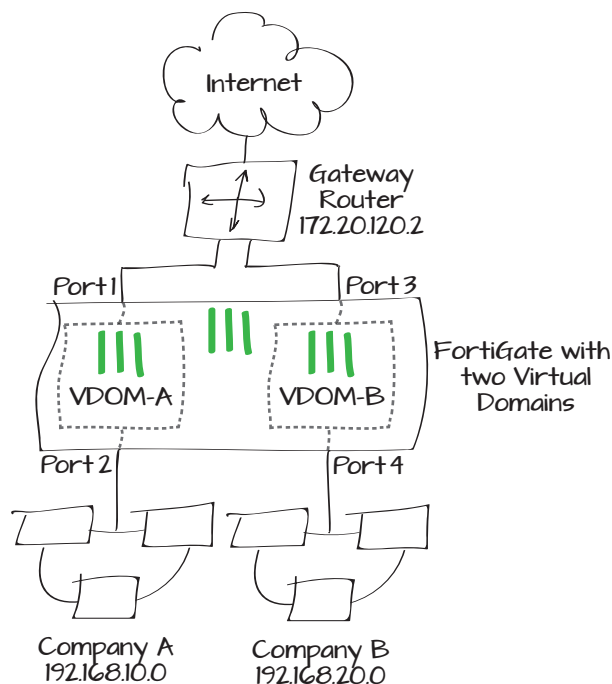


Resetting the FortiGate unit to factory defaults will put the unit back into NAT/Route mode.

# Using VDOMs to host two FortiOS instances on a single FortiGate unit

Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct Internet services. Each company has its own VDOM, IP address, and internal network.

1. Switching to VDOM mode and creating two VDOMS
2. Assigning interfaces to each VDOM
3. Creating administrators for each VDOM
4. Creating a basic configuration for VDOM-A
5. Creating a basic configuration for VDOM-B
6. Connecting the gateway router
7. Results



## Switching to VDOM mode and creating two VDOMS

Go to **System > Dashboard > Status**.

In the **System Information** widget, find **Virtual Domain** and select **Enable**.



You will be required to re-login after enabling **Virtual Domain** due to the GUI menu options changing.

Go to **Global > VDOM > VDOM**.

Create two VDOMS: *VDOM-A* and *VDOM-B*.  
Leave both VDOMs as **Enabled**, with **Operation Mode** set to **NAT**.

System Information	
Host Name	FG100D3G12812324 [Change]
Serial Number	FG100D3G12812324
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Wed Oct 30 06:28:30 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0246 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	2 day(s) 0 hour(s) 46 min(s)
Virtual Domain	Disabled [Enable]

Name	<input type="text" value="VDOM-A"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Name	<input type="text" value="VDOM-B"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

# Assigning interfaces to each VDOM

Go to **Global > Network > Interfaces**.

Edit **port1** and add it to VDOM-A. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, 172.20.120.10/255.255.255.0).

Edit **port2** and add it to VDOM-A. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, 192.168.10.1/255.255.255.0), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.

Edit **port3** and add it to VDOM-B. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, 172.20.120.20/255.255.255.0).

Name

port1(00:09:0F:B0:EB:F0)

Alias

Link Status

Down

Type

Physical Interface

Virtual Domain

VDOM-A

Addressing mode

Manual

IP/Network Mask

172.20.120.10/255.255.255.0

IPv6 Address

:::0

Name

port2(00:09:0F:B0:EB:F1)

Alias

Link Status

Down

Type

Physical Interface

Virtual Domain

VDOM-A

Addressing mode

Manual

IP/Network Mask

192.168.10.1/255.255.255.0

IPv6 Address

:::0

Administrative Access

HTTPS

SSH

PING

SNMP

HTTP

TELNET

FMG-Access

FCT-Access

CAPWAP

IPv6 Administrative Access

HTTPS

SSH

PING

SNMP

HTTP

TELNET

FMG-Access

FCT-Access

CAPWAP

DHCP Server

Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
192.168.10.2	192.168.10.254

Netmask

255.255.255.0

Name

port3(00:09:0F:B0:EB:F2)

Alias

Link Status

Down

Type

Physical Interface

Virtual Domain

VDOM-B

Addressing mode

Manual

IP/Network Mask

172.20.120.20/255.255.255.0

IPv6 Address

:::0

Edit **port4** and add it to VDOM-B. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, 192.168.20.1/255.255.255.0), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.

# Creating administrators for each VDOM

Go to **Global > Admin > Administrators**.

Create an administrator for VDOM-A, called *a-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof\_admin**.

Create an administrator for VDOM-B, called *b-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof\_admin**.



Make sure to remove the **root** VDOM from both administrator accounts.

Name

port4(00:09:0F:B0:EB:F3)

Alias

Link Status

Down

Type

Physical Interface

Virtual Domain

VDOM-B

Addressing mode

Manual

DHCP

PPPoE

One-Arm Sniffer

Dedicate to FortiAP/FortiSwitch

IP/Network Mask

192.168.20.1/255.255.255.0

IPv6 Address

:::/0

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☐ FMG-Access

☐ CAPWAP

☒ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ CAPWAP

☐ SSH

☐ SNMP

☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
192.168.20.2	192.168.20.254

Netmask

255.255.255.0

Administrator

a-admin

Type

Regular

Remote

PKI

Password

.....

Confirm Password

.....

Comments

Write a comment...

0/255

Admin Profile

prof\_admin

Virtual Domain

VDOM-A

Administrator

b-admin

Type

Regular

Remote

PKI

Password

.....

Confirm Password

.....

Comments

Write a comment...

0/255

Admin Profile

prof\_admin

Virtual Domain

VDOM-B

## Creating a basic configuration for VDOM-A

Go to **Virtual Domains** and select **VDOM-A**.

Go to **Router > Static > Static Routes**.

Add a default route for the VDOM. Set **Destination IP/Mask** to `0.0.0.0/0.0.0.0`, set **Device** to **port1**, and set **Gateway** to the IP of the gateway router (in the example, `172.20.120.2`).

Connect a PC to port2. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-A using the a-admin account (in the example, `https://192.168.10.1`).

Go to **Policy > Policy > Policy**.

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Select **Enable NAT**.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="port1"/>
Gateway	<input type="text" value="172.20.120.2"/>

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	<input type="text" value="port2"/>
Source Address	<input type="text" value="all"/>
Outgoing Interface	<input type="text" value="port1"/>
Destination Address	<input type="text" value="all"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input type="text" value="ACCEPT"/>
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
<input data-bbox="997 1266 1355 1289" type="text" value="Click to add..."/>	

## Creating a basic configuration for VDOM-B

If you have logged out of the FortiGate unit, log back in.

Go to **Virtual Domains** and select **VDOM-B**. Go to **Router > Static > Static Routes**.







Add a default route for the VDOM. Set **Destination IP/Mask** to `0.0.0.0/0.0.0.0`, set **Device** to **port3**, and set **Gateway** to the IP of the gateway router (in the example, `172.20.120.2`).

Connect a PC to port4. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-B using the b-admin account (in the example, `https://192.168.20.1`).

Go to **Policy > Policy > Policy**.

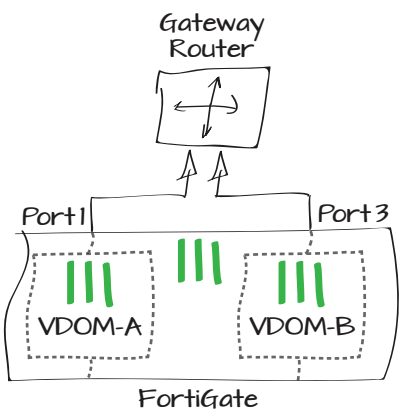
Create a policy to allow Internet access. Set **Incoming Interface** to **port4** and **Outgoing Interface** to **port3**. Select **Enable NAT**.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="port3"/>
Gateway	<input type="text" value="172.20.120.2"/>

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	<input type="text" value="port4"/> 
Source Address	<input type="text" value="all"/> 
Outgoing Interface	<input type="text" value="port3"/> 
Destination Address	<input type="text" value="all"/> 
Schedule	<input type="text" value="always"/> 
Service	<input type="text" value="ALL"/> 
Action	<input type="text" value="ACCEPT"/>
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="radio"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
<input type="text" value="Click to add..."/>	

# Connecting the gateway router

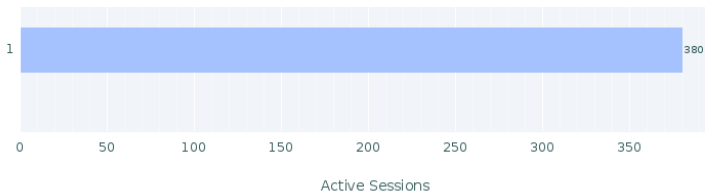
Connect port1 and port3 of the FortiGate unit to the gateway router to allow Internet traffic to flow.



## Results

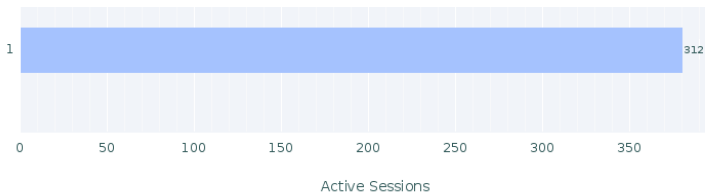
Connect to the Internet from the company A and company B networks and then log into the FortiGate unit.

Go to **Virtual Domains** and select **VDOM-A**. Go to **Policy > Policy > Monitor** to view the sessions being processed on VDOM-A.



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions
1	port2	port1	✓	380

Go to **Virtual Domains** and select **VDOM-B**. Go to **Policy > Policy > Monitor** to view the sessions being processed on VDOM-B.



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions
1	port4	port3	✓	312



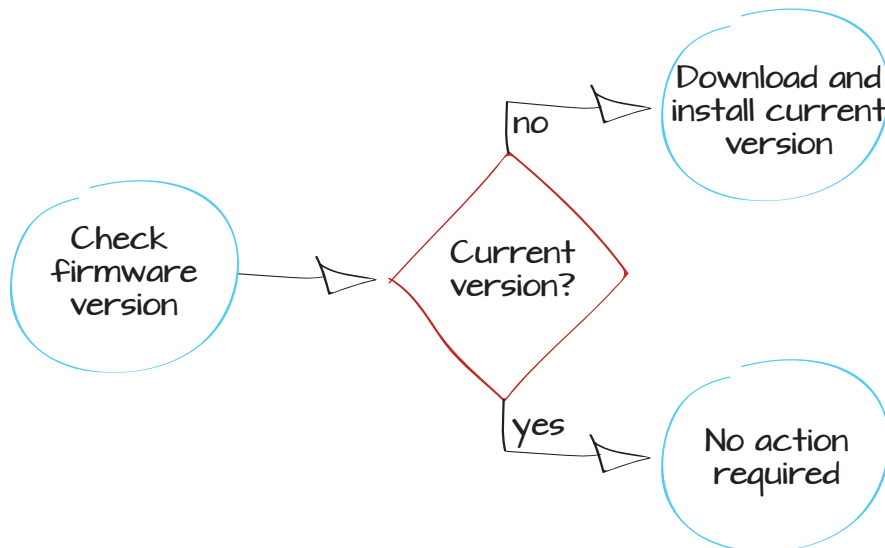
# Verifying and updating the FortiGate unit's firmware

This example verifies the current version of FortiOS firmware and, if necessary, updates it to the latest version.



Always review the Release Notes before installing a new firmware version. They provide the recommended upgrade path for the firmware release as well as additional information not available in other documentation. Only perform a firmware update during a maintenance window.

1. Checking the current FortiOS firmware
2. Downloading the latest FortiOS firmware
3. Updating the FortiGate to the latest firmware
4. Results



# Checking the current FortiOS firmware

Log in to the web-based manager and view the dashboard **System Information** widget to see the **Firmware Version** currently installed on your FortiGate unit.

# Downloading the latest FortiOS firmware

To download a newer firmware version, browse to <http://support.fortinet.com> and log in using your Fortinet account user name and password.



Your FortiGate unit must be registered before you can access firmware images from the Support site.

Go to **Download Firmware Images > FortiGate**. Locate and download the firmware for your FortiGate unit.

Download and read the Release Notes for this firmware version. Always review the Release Notes before installing a new firmware version in case you cannot update to the new firmware release from the one currently running.

System Information	
Host Name	FG100D3G12801345 [Change]
Serial Number	FG100D3G12801345
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Fri Aug 23 11:14:41 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0228 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	14 day(s) 5 hour(s) 48 min(s)
Virtual Domain	Disabled [Enable]



- Download**
- > [FortiGuard Service Updates](#)
  - > [Firmware Images](#)
  - > [Firmware Image Checksums](#)

Please select from the products listed below for Firmware Downloads:	
» <a href="#">FortiADC</a> » <a href="#">FortiADC-E</a> » <a href="#">FortiAnalyzer</a> » <a href="#">FortiAP</a> » <a href="#">FortiAuthenticator</a> » <a href="#">FortiBalancer</a> » <a href="#">FortiBridge</a> » <a href="#">FortiCache</a> »	
<a href="#">FortiCarrier</a> » <a href="#">FortiClient</a> » <a href="#">FortiClientMac</a> » <a href="#">FortiConverter</a> » <a href="#">FortiDB</a> » <a href="#">FortiDDoS</a> » <a href="#">FortiDNS</a> » <a href="#">FortiExplorer</a> » <a href="#">FortiGate</a> »	
<a href="#">FortiGate-One</a> » <a href="#">FortiLog</a> » <a href="#">FortiMail</a> » <a href="#">FortiManager</a> » <a href="#">FortiRecorder</a> » <a href="#">FortiScan</a> » <a href="#">FortiSwitch</a> » <a href="#">FortiSwitchATCA</a> » <a href="#">FortiToken</a> »	
» <a href="#">FortiVoice</a> » <a href="#">FortiVoiceOS</a> » <a href="#">FortiWeb</a> » <a href="#">TalkSwitch</a>	
The checksums to all images are stored <a href="#">HERE</a>	

Index of <ftp://pftpintl@support.fortinet.com/FortiGate/v5.00/5.0/5.0.4/>

[Up to higher level directory](#)

Name	Size	Last Modified
<a href="#">FGR_100C-v500-build0228-FORTINET.out</a>	28248 KB	2013-08-12 11:32:00 PM
<a href="#">FGT_1000C-v500-build0228-FORTINET.out</a>	31786 KB	2013-08-09 11:34:00 PM
<a href="#">FGT_100D-v500-build0228-FORTINET.out</a>	31328 KB	2013-08-09 11:33:00 PM
<a href="#">FGT_110C-v500-build0228-FORTINET.out</a>	25265 KB	2013-08-09 11:33:00 PM
<a href="#">FGT_111C-v500-build0228-FORTINET.out</a>	26780 KB	2013-08-09 11:33:00 PM
<a href="#">FGT_1240B-v500-build0228-FORTINET.out</a>	32958 KB	2013-08-09 11:34:00 PM

## Updating the FortiGate to the latest firmware

Go to **System > Dashboard > Status**.

Backup your configuration from the **System Information** dashboard widget, next to **System Configuration**..



Always remember to back up your configuration before doing any firmware upgrades.

Under **System Information > Firmware Version**, select **Update**.

Find the firmware image file that you downloaded and select **OK** to upload and install the firmware build on the FortiGate unit.

## Results

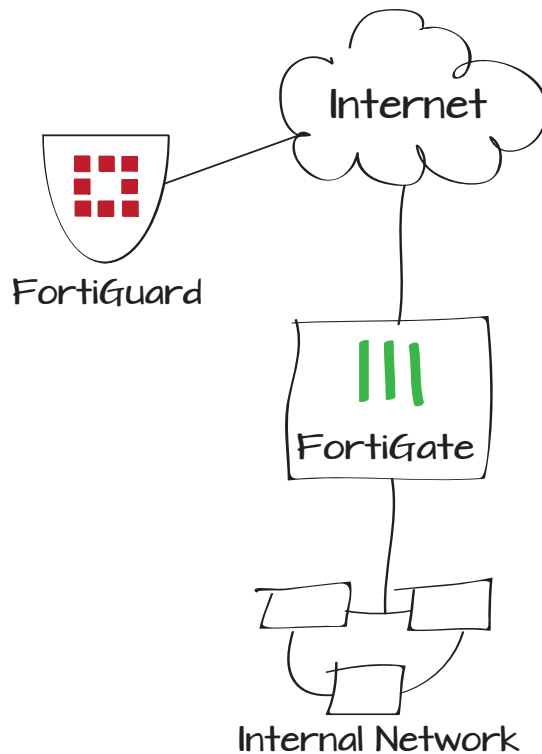
The FortiGate unit uploads the firmware image file, updates to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

From the FortiGate web-based manager, go to **System > Dashboard > Status**. In the **System Information** widget, the Firmware Version will show the updated version of FortiOS.

System Information	
Host Name	FG100D3G12801345 [Change]
Serial Number	FG100D3G12801345
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Fri Aug 23 11:14:41 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0228 (Interim) [Update] [Details]
System Configuration	[Backup] Restore [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	14 day(s) 5 hour(s) 48 min(s)
Virtual Domain	Disabled [Enable]

# Setting up FortiGuard services

If you have purchased FortiGuard services and registered your FortiGate unit, the FortiGate should automatically connect to a FortiGuard Distribution Network (FDN) and display license information about your FortiGuard services. In this example, you will verify whether the FortiGate unit is communicating with the FDN by checking the License Information dashboard widget.



## Verifying the connection

On the dashboard, go to the **License Information** widget.

Any subscribed services should have a green check mark, indicating that connections are successful.

A grey X indicates that the FortiGate unit cannot connect to the FortiGuard network, or that the FortiGate unit is not registered.

A red X indicates that the FortiGate unit was able to connect but that a subscription has expired or has not been activated.

You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.

License Information		
<b>Support Contract</b>		
Registration	Registered (Login: vancouver_support@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2013-12-10)	✓
Firmware	8 x 5 support (Expires: 2013-12-10)	✓
Enhanced Support	24 x 7 support (Expires: 2013-12-10)	✓
Comprehensive Support	24 x 7 support (Expires: 2013-12-10)	✓
<b>FortiGuard Services</b>		
AntiVirus	Licensed (Expires 2013-12-10)	✓
IPS & Application Control	Licensed (Expires 2013-12-10)	✓
Vulnerability Scan	Licensed (Expires 2013-12-10)	✓
Web Filtering	Licensed (Expires 2013-12-09)	✓
Email Filtering	Licensed (Expires 2013-12-09)	✓

<b>Support Contract</b>		
Registration	Registered (Login ID: vancouver_support@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2013-12-10)	✓
Firmware	8 x 5 support (Expires: 2013-12-10)	✓
Enhanced Support	24 x 7 support (Expires: 2013-12-10)	✓
Comprehensive Support	24 x 7 support (Expires: 2013-12-10)	✓
<b>FortiGuard Subscription Services</b>		
AntiVirus	Valid License (Expires 2013-12-10)	✓
AV Definitions	1.00000 (Updated 2012-10-17 via Manual Update) [Update]	
AV Engine	5.00032 (Updated 2012-10-16 via Manual Update)	
IPS & Application Control	Valid License (Expires 2013-12-10)	✓
IPS Definitions	4.00295 (Updated 2013-01-28 via Manual Update) [Update]	
IPS Engine	2.00132 (Updated 2013-02-20 via Manual Update)	
Vulnerability Scan	Valid License (Expires 2013-12-10)	✓
VCM Plugins	1.00297-L (Updated 2013-03-04 via Manual Update) [Update]	
VCM Engine	1.00297 (Updated 2013-03-04 via Manual Update)	
Web Filtering	Valid License (Expires 2013-12-09)	✓
Email Filtering	Valid License (Expires 2013-12-09)	✓
Messaging Services	Unreachable	✗

# Extra help: FortiGuard

This section contains tips to help you with some common challenges of using FortiGuard.

## FortiGuard services appear as expired/unreachable.

Verify that you have registered your FortiGate unit, purchased FortiGuard services and that the services have not expired at [support.fortinet.com](https://support.fortinet.com).

## Services are active but still appear as expired/unreachable.

Verify that the FortiGate unit can communicate with the Internet.

## The FortiGate is connected to the Internet but can't communicate with FortiGuard.

Go to **System > Network > DNS** and ensure that the primary and secondary DNS servers are correct. If the FortiGate interface connected to the Internet gets its IP address using DHCP, make sure **Override internal DNS** is selected.

Also, determine if the default port used for FortiGuard traffic, port 53, is being blocked, either by a device on your network or by your ISP. If you cannot unblock the port, change it by going to **System > Config > FortiGuard** and selecting the service(s) where communication errors are occurring. Under **Port Selection**, select **Use Alternate Port**.

## Communication errors remain.

FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets.

In effort to avoid port blocking, You can configure your FortiGate unit to use higher-numbered ports, such as 2048-20000, using the following CLI command:

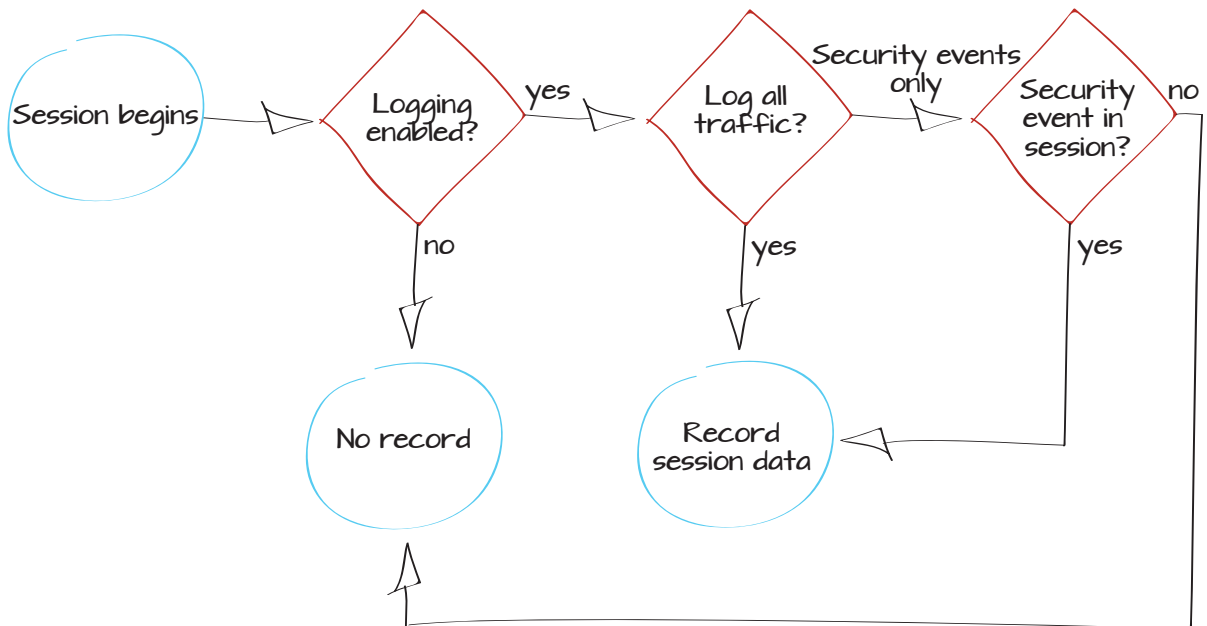
```
config system global
    set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use.

# Logging network traffic to gather information

This example demonstrates how to enable logging to capture the details of the network traffic processed by your FortiGate unit.

1. Recording log messages and enabling event logging
2. Enabling logging in the security policies
3. Results



## Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**.

Select where log messages will be recorded. You can save log messages to disk if your FortiGate unit supports this, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create reports based on them.

In most cases, it is recommended to **Send Logs to FortiCloud**, as shown in the example. For more information on FortiCloud, see [“Using FortiCloud to record log messages”](#) on page 44.

Next, enable **Event Logging**.

You can choose to **Enable All** types of logging, or specific types, such as **WiFi activity events**, depending on your needs.

### Logging and Archiving

☐ Disk

☐ Send Logs to FortiAnalyzer/FortiManager

IP Address:

Test Connectivity

☒ Send Logs to FortiCloud

Account:

email@example.com

Test Connectivity

Upload Option

☒ Realtime

☒ Event Logging

☒ Enable All

☒ WiFi activity event

☒ System activity event

☒ User activity event

☒ Router activity event

☒ VPN activity event

☒ Explicit web proxy event

### GUI Preferences

Display Logs From

FortiCloud

☒ Resolve Hostnames (Using reverse DNS lookup)

☒ Resolve Unknown Applications (Using remote application database)

Apply



# Enabling logging in the security policies

Go to **Policy > Policy > Policy**. Edit the policies controlling the traffic you wish to log.

Under **Logging Options**, you can choose either **Log Security Events** or **Log all Sessions**.

In most cases, you should select **Log Security Events**. **Log all Sessions** can be useful for more detailed traffic analysis but also has a greater effect on system performance and requires more storage.

## Results

View traffic logs by going to **Log & Report > Traffic Log > Forward Traffic**. The logs display a variety of information about your traffic, including date/time, source, device, and destination.

To change the information shown, right-click on any column title and select **Column Settings** to enable or disable different columns.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Fixed Port

Click to add...

☒ Firewall

☐ VPN

☒ Address

☐ User Identity

☐ Device Identity

internal

+

all

+

wan1

+

all

+

always

▼

ALL

+

ACCEPT

▼

































Logging Options

☐ No Log





☐ Log Security Events

☒ Log all Sessions

Download Raw Log

Time	Src	Device	Dst	Application Name	Sent / Received
192.168.1.117	 00:0c:29:c2:38:8e	 208.91.113.70	 NTP	608 B / 608 B	
192.168.1.117	 00:0c:29:c2:38:8e	 208.91.112.53	 DNS	43.06 KB / 93.73 KB	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.113.184	 Unknown	120 B / 0 B	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.112.53	 DNS	536 B / 777 B	
192.168.1.117	 00:0c:29:c2:38:8e	 208.91.112.50	 NTP	912 B / 912 B	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.113.184	 Unknown	120 B / 0 B	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.113.184	 Unknown	120 B / 0 B	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.112.53	 DNS	670 B / 1.08 KB	
192.168.1.117	 00:0c:29:c2:38:8e	 208.91.113.70	 NTP	1.48 KB / 1.48 KB	
192.168.1.100	 00:09:0f:7e:71:fe	 208.91.113.184	 Unknown	120 B / 0 B	
192.168.1.114	 00:0c:29:4b:d7:cc	192.168.110.9	 Unknown	77 B / 389 B	























You can also select any entry to view more information about a specific session.



Dst	 208.91.113.184	Virtual Domain	root
Received	0	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	120 B / 0 B
Device Type	Fortinet Device	Duration	123
Sent	120	Src NAT Port	62620
Application Details		Device	 00:09:0f:7e:71:fe
Service	HTTPS	Protocol	6
byod_name		Destination Country	Canada
Dst Port	443	roll	65406
Status	timeout	Timestamp	Mon Mar 11 10:36:43 2013
Tran Display	snat	OS Name	Fortinet OS
Sequence Number	954732	Policy ID	3
Src Interface	port1	Src	192.168.1.100
Sent Packets	2	Level	notice  
Src Port	2204	Log ID	13
Sub Type	forward	Threat	
Received Packets	0	Date/Time	10:36:43 (Mon Mar 11 10:36:43 2013)
Dst Interface	wan1		

Different types of event logs can be found at **Log & Report > Event Log**.

The example shows the System log that records system events, such as administrative logins and configuration changes.

As with the Forward Traffic log, select an entry for further information.

Refresh Download Raw Log				Log 1
#	Date/Time	Level	User	Message
1	11:46:49		admin	Administrator admin logged in successfully from http(127.0.0.1)
2	11:42:45			Performance statistics
3	11:39:52			Interface wan1 gets a DHCP lease, ip:172.20.120.234, mask:255.255.255.0, gateway:172.20.120.2, lease expires:Tue Jul 2 12:39:48 2013
4	11:37:45			Performance statistics
5	11:32:45			Performance statistics
6	11:27:45			Performance statistics
7	11:22:45			Performance statistics
8	11:17:45			Performance statistics
9	11:12:45			Performance statistics
10	11:09:52			Interface wan1 gets a DHCP lease, ip:172.20.120.234, mask:255.255.255.0, gateway:172.20.120.2, lease expires:Tue Jul 2 12:09:48 2013
11	11:07:45			Performance statistics
12	11:02:45			Performance statistics
13	10:57:45			Performance statistics
14	10:53:13		admin	Administrator admin timed out on https(192.168.1.110)
15	10:52:45			Performance statistics
16	10:47:51		admin	Administrator admin timed out on https(192.168.1.110)
17	10:47:51		admin	Administrator admin logged in successfully from https(192.168.1.110)
18	10:47:45			Performance statistics
19	10:42:45			Performance statistics
20	10:39:52			Interface wan1 gets a DHCP lease, ip:172.20.120.234, mask:255.255.255.0, gateway:172.20.120.2, lease expires:Tue Jul 2 11:39:48 2013
21	10:37:45			Performance statistics
22	10:32:45			Performance statistics

Virtual Domain	root	Level	notice  
Memory	68	Timestamp	Tue Jul 2 11:37:45 2013
CPU	0	Log ID	40704
Sub Type	system	Total Sessions	43
Action	perf-stats	Date/Time	11:37:45 (Tue Jul 2 11:37:45 2013)
Message	Performance statistics		

# Extra help: Logging

This section contains tips to help you with some common challenges of FortiGate logging.

## No log messages appear.

Ensure that logging is enabled in both the **Log Settings** and the policy used for the traffic you wish to log, as logging will not function unless it is enabled in both places.

If logging is enabled in both places, check that the policy in which logging is enabled is the policy being used for your traffic. Also make sure that the policy is getting traffic by going to the policy list and adding the **Sessions** column to the list.

## Logs from a FortiAnalyzer, FortiManager, or from FortiCloud do not appear in the GUI.

Ensure that the correct log source has been selected in the **Log Settings**, under **GUI Preferences**.

## The FortiGate unit's performance level has decreased since enabling disk logging.

If enabling disk logging has impacted overall performance, change the log settings to either send logs to a FortiAnalyzer unit, a FortiManager unit, or to FortiCloud.

## Log All Sessions is enabled on all security policies and cannot be changed.

This can occur if **Client Reputation** is enabled.

## Logging to a FortiAnalyzer unit is not working as expected.

The firmware for the FortiGate and FortiAnalyzer units may not be compatible. Check the firmware release notes, found at [support.fortinet.com](https://support.fortinet.com), to see if this is the case.

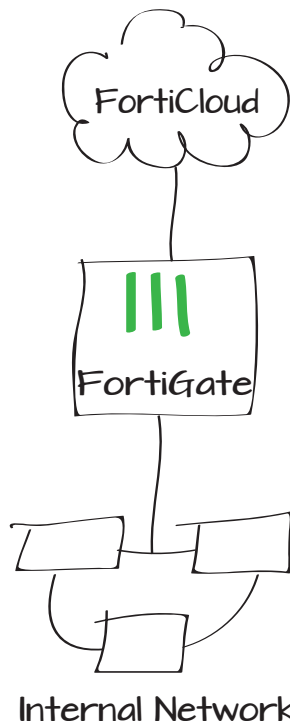
# Using FortiCloud to record log messages

This example describes setting up FortiGate logging to FortiCloud, an online log retention service provided by Fortinet. It also describes how to use FortiCloud to view and access FortiGate traffic logs.



You must register your FortiGate unit before you can activate FortiCloud.

1. Activating FortiCloud
2. Sending logs to FortiCloud
3. Enabling logging in your security policies
4. Results



# Activating FortiCloud

Go to **System > Dashboard > Status**.

In the **FortiCloud** section of the **License Information** widget, select the green **Activate** button.

Fill in the required information to create a new FortiCloud account.

License Information

Support Contract

Registration	Registered (Login: Imullen@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2014-05-24)	✓
Firmware	8 x 5 support (Expires: 2014-05-24)	✓
Enhanced Support	24 x 7 support (Expires: 2014-05-24)	✓
Comprehensive Support	24 x 7 support (Expires: 2014-05-24)	✓

FortiGuard Services

Next Generation Firewall

IPS & Application Control	Licensed (Expires 2014-05-24)	✓
---------------------------	-------------------------------	---

ATP Services

AntiVirus	Licensed (Expires 2014-05-24)	✓
Web Filtering	Licensed (Expires 2014-05-23)	✓

Other Services

Vulnerability Scan	Licensed (Expires 2014-05-24)	✓
Email Filtering	Licensed (Expires 2014-05-23)	✓

FortiCloud

Account	Activate
---------	----------

FortiClient Software

Mac Windows

Registered/Allowed	0 of 10	[Details] [Enter License]
--------------------	---------	---------------------------

FortiToken Mobile

Assigned/Allowed	0 of 2
------------------	--------

Activate FortiCloud

☐ Login

☒ Create Account

Please enter the information below and click the activate button

Email:

admin@company.com

Re-type email:

admin@company.com

Password:

••••••••

Re-type Password:

••••••••

☒ I Agree to the FortiCloud Terms & Conditions [View]

## Sending logs to FortiCloud

Go to **Log & Report > Log Config > Log Setting**.

Enable **Send Logs to FortiCloud** and adjust the **Event Logging** settings as required.

Select **Test Connectivity** to verify the connection between the FortiGate unit and your FortiCloud account.

Set the **GUI Preferences** to **Display Logs from FortiCloud**, to easily view your logs.

### Logging and Archiving

☒ Disk

☐ Send Logs to FortiAnalyzer/FortiManager

IP Address:

☒ Send Logs to FortiCloud

Account:

Upload Option

☒ Realtime

☒ Event Logging

☒ Enable All

☒ WiFi activity event

☒ System activity event

☒ User activity event

☒ Router activity event

☒ VPN activity event

☒ Explicit web proxy event

### GUI Preferences

Display Logs From

☒ Resolve Hostnames (Using reverse DNS lookup)

☒ Resolve Unknown Applications (Using remote application database)

## Enabling logging in the security policies

Go to **Policy > Policy > Policy**. Edit the security policies that control the traffic you wish to log.

Under **Logging Options**, select either **Log Security Events** or **Log all Sessions**, depending on your needs.

In most cases, **Log Security Events** will provide sufficient information in the traffic logs. **Log all Sessions** can be useful for more detailed traffic analysis but also has a greater effect on system performance and requires more memory for storage.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

### Logging Options

☐ No Log

☒ Log Security Events

☐ Log all Sessions

## Results

Go to **System > Dashboard > Status**.

In the **FortiCloud** section of the **License Information** widget, select **Launch Portal**.

From the portal, you can view the log data and reports.

You can access your FortiCloud account at any time by going to [www.forticloud.com](http://www.forticloud.com).

Daily Summary reports can also be found through the FortiGate unit by going to **Log & Report > Report > FortiCloud**.

You can also configure your FortiCloud account to have these reports emailed to you.

Logs viewed through the GUI will also now read **Log location: FortiCloud** in the upper right corner.

FortiCloud

Dashboards Logs & Archives Drilldown Reports Management

Logs & Archives

Device: FG100D3G12804195

Traffic Log - FG100D3G12804195

Refresh Column Settings Clear Filters Period: Last 7 days Formatted Raw

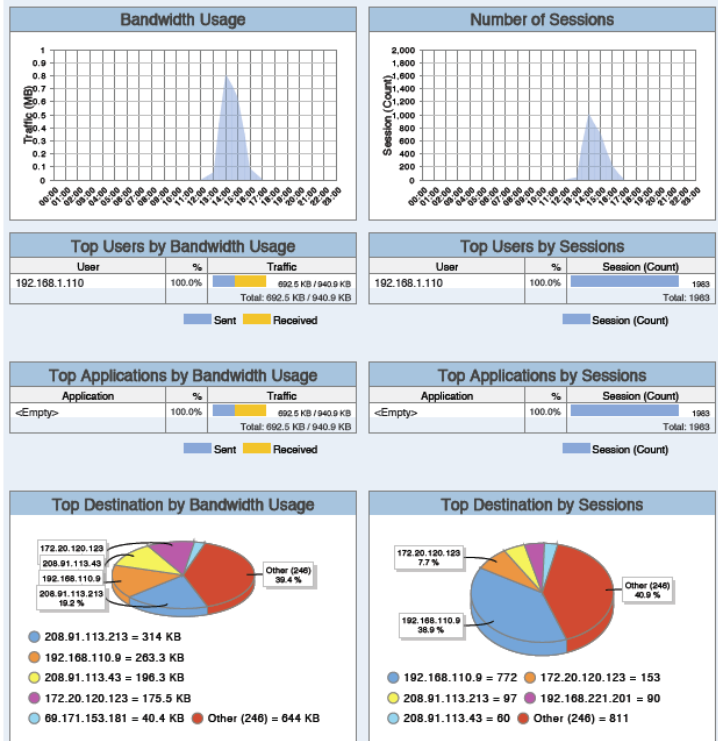
#	Time	Level	Service	Source	Destination	Sent
1	2013-03-27 05:44:38	OK	8010/tcp	192.168.1.111	192.168.1.99	0
2	2013-03-27 05:44:38	OK	8612/udp	172.20.120.14	172.20.120.255	0
3	2013-03-27 05:44:38	OK	8612/udp	172.20.120.14	224.0.0.1	0
4	2013-03-27 05:44:37	OK	8010/tcp	192.168.1.200	192.168.1.99	0
5	2013-03-27 05:44:36	OK	8612/udp	172.20.120.83	172.20.120.255	0
6	2013-03-27 05:44:36	OK	8612/udp	172.20.120.83	224.0.0.1	0
7	2013-03-27 05:44:34	OK	DCE-RPC	192.168.1.111	208.91.113.213	800
8	2013-03-27 05:44:33	OK	HTTPS	192.168.1.111	208.91.113.96	5889
9	2013-03-27 05:44:33	OK	HTTPS	192.168.1.111	208.91.113.96	6305
10	2013-03-27 05:44:33	OK	HTTPS	192.168.1.111	208.91.113.96	5953
11	2013-03-27 05:44:33	OK	HTTPS	192.168.1.111	208.91.113.96	5889
12	2013-03-27 05:44:33	OK	HTTPS	192.168.1.111	208.91.113.96	4615
13	2013-03-27 05:44:32	OK	HTTPS	192.168.1.111	65.54.52.250	944
14	2013-03-27 05:44:31	OK	8612/udp	172.20.120.14	224.0.0.1	0
15	2013-03-27 05:44:31	OK	8612/udp	172.20.120.14	172.20.120.255	0

1

\* click anywhere in a row to view details.

### Summary Report

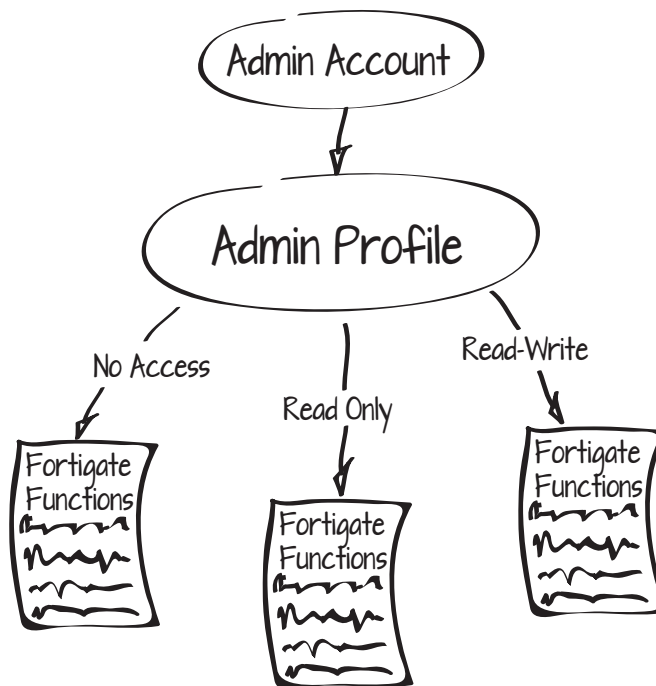
#### Bandwidth and Applications



# Setting up a limited access administrator account

This example adds a new FortiGate administrator account that uses an administrative profile with access limited to read and write for authentication and device information and to reading for logs and reports. Account access to the firewall will be limited to connections from a specific subnet.

1. Creating a new administrative profile
2. Adding a new administrator and assigning the profile
3. Results





# Creating a new administrative profile

Go to **System > Admin > Admin Profile**.

Create a new administer profile that allows the administrator with this profile to view and edit components of **User and Devices** and to view logs and reports.

Profile Name:

Comments:  72/255

☐ None ☐ Read Only ☐ Read-Write

System Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Admin Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiGuard Update	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Router Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Profile Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
User & Device	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
WAN Opt & Cache	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Endpoint Security	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
WiFi Controller	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Log & Report	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Report Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

# Adding a new administrator and assigning the profile

Go to **System > Admin > Administrators**.

Create a new administrator account and assign it to the profile new that was just created.

Restrict access to the firewall to logins from Trusted Hosts Only by adding the IP address range to one of the **Trusted Host** fields.

## Results

Log in to the FortiGate unit using the user name of new administrator account.

The admin profile controls what features of the FortiGate configuration the administrator can see and configure from web-based manager and CLI.

This administrator can create and edit elements regarding users, authentication and

Administrator

t.white

Type

Regular

Remote

PKI

Password

.....

Confirm Password

.....

Comments

Authentication Manager

22/255

Admin Profile

Authentication\_Management

Contact Info

Email Address

t.white@example.com

SMS

FortiGuard Messaging Service

Custom

Phone Number

Enable Two-factor Authentication

Restrict this Admin Login from Trusted Hosts Only

Trusted Host #1

172.20.120.0/24

Trusted Host #2

0.0.0.0/0.0.0.0

Trusted Host #3

0.0.0.0/0.0.0.0

IPv6 Trusted Host #1

::/0

IPv6 Trusted Host #2

::/0

IPv6 Trusted Host #3

::/0

Restrict to Provision Guest Accounts

System

User & Device

User

User Definition

User Group

Guest Management

Device

Authentication

Two-factor Authentication

Vulnerability Scan

Monitor

Create New

Edit User

Search

User Name	Type	Two-factor Authentication	Ref.
George	LOCAL	<div></div>	3
John	LOCAL	<div></div>	3
Paul	LOCAL	<div></div>	4
Ringo	LOCAL	<div></div>	3
Yoko	LOCAL	<div></div>	0
guest	LOCAL	<div></div>	1

devices etc. Also available for viewing are the logs and reports. Elements not specified as Readable do not appear.

Log in with a super admin account.

Go to **System > Dashboard > Status**, and view the System Information widget.

Select **Details** for the Current Administrator to view all administrators logged in.

Go to **Log & Report > Event Log > System**.

The upper pane will show the activity, such as the successful login of the t.white admin account.

Select the entry for the new administrator login to get more detailed information to show in the lower pane.

The details show that the new administrator account logged in from an IP address that is within the ranges specified in the **Trusted Hosts** field.

System Information	
Host Name	FG100D3G12804410 [Change]
Serial Number	FG100D3G12804410
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Thu Sep 5 17:05:03 2013 [Change]
Firmware Version	v5.0,build0228 (GA Patch 4) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /5 in Total [Details]
Uptime	6 day(s) 2 hour(s) 13 min(s)
Virtual Domain	Disabled [Enable]

Administrators logged in				
<input type="checkbox"/>	User Name	Access Profile	Type	From
<input type="checkbox"/>	admin	super_admin	https	192.168.150.50 Thu Sep 5 15:45:36 2013
<input type="checkbox"/>	t.white	Authentication_Management	https	172.20.120.229 Thu Sep 5 16:20:21 2013
<input type="checkbox"/>	admin	super_admin	https	172.20.120.229 Thu Sep 5 16:21:59 2013

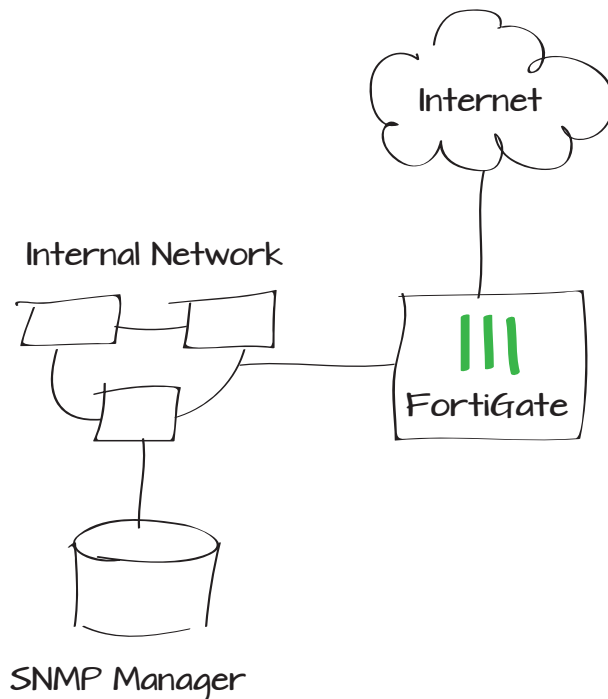
#	Date/Time	Level	User	Message
16	16:20:21		t.white	Administrator t.white logged in successfully from https(172.20.120.229)
17	16:16:50			Performance statistics
18	16:11:50			Performance statistics
19	16:06:51			Performance statistics
1 / 55 [ Total: 2726 ]				
Action	login	Date/Time	16:20:21 (137839802	
Level	information	Log ID	32001	
Message	Administrator t.white logged in successfully from https(172.20.120.229)	Profile Name	Authentication_Manag	
Reason	none	Status	success	
Sub Type	system	Timestamp	Thu Sep 5 16:20:21 2	
User	t.white	User Interface	https(172.20.120.229	

# Using SNMP to monitor the FortiGate unit

The Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers.

In this example, you configure the FortiGate SNMP agent and an example SNMP manager so that the SNMP manager can get status information from the FortiGate unit and so that the FortiGate unit can send traps to the SNMP manager.

1. Configuring the FortiGate SNMP agent
2. Enabling SNMP on a FortiGate interface
3. Downloading Fortinet MIB files to and configuring an example SNMP manager
4. Results



# Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**.

Configure the SNMP agent.

SNMP Agent

☒ Enable

Description

Company FortiGate unit

Location

Head Office, server room

Contact

admin@company.com

Apply

SNMP v1/v2c

Create New

Edit

Delete

	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	FortiGates	✓	✓	<input checked="" type="checkbox"/>

SNMP v3

Create New

Edit

Delete

	User Name	Security Level	Notification Host	Queries
--	-----------	----------------	-------------------	---------

FortiGate SNMP MIB

[Download FortiGate MIB File](#)

[Download Fortinet Core MIB File](#)

Under **SNMP v1/v2c** create a new community.

Add the IP address of SNMP manager (in the example, 192.168.1.114/32). If required, change the query and trap ports to match the SNMP manager.

You can add multiple SNMP managers or set the IP address/Netmask to 0.0.0.0/0.0.0.0 and the Interface to ANY so that any SNMP manager on any network connected to the FortiGate unit can use this SNMP community and receive traps from the FortiGate unit.

Enable the **SNMP Events** (traps) that you need. In most cases leave them all enabled.

## Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces**.

Enable SNMP administrative access on the interface connected to the same network as the SNMP manager.

Edit SNMP Community

Community NameFortiGates

Hosts:

IP Address/Netmask	Interface	Delete
192.168.1.114/255.255.255.255	port1	

Add

Queries:

Protocol	Port	Enable
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>

Traps:

Protocol	Local	Remote	Enable
v1	162	162	<input checked="" type="checkbox"/>
v2c	162	162	<input checked="" type="checkbox"/>

SNMP Events

☒ CPU usage is high

☒ Log disk space is low

☒ VPN tunnel up

☒ WiFi Controller AP up

☒ FortiSwitch Controller Session up

☒ HA cluster status is changed

☒ HA member up

☒ Virus detected

☒ Fragmented email detected

☒ Oversized file/email blocked

☒ AV bypass happens

☒ IPS anomaly detected

☒ IPS package updated

☒ System enters conserve mode

☒ FortiAnalyzer disconnected

☒ Memory is low

☒ Interface IP is changed

☒ VPN tunnel down

☒ WiFi Controller AP down

☒ FortiSwitch Controller Session down

☒ HA heartbeat failure

☒ HA member down

☒ Matched file pattern detected

☒ Oversized file/email detected

☒ Oversized file/email passed

☒ IPS attack detected

☒ System configuration is changed

Name

port1 (00:09:0F:4E:10:1F)

Alias

Link Status

Up

Addressing mode

☒ Manual

☐ DHCP

☐ Dedicate to FortiAP/FortiSwitch

IP/Network Mask:

192.168.1.99/255.255.255.0

IPv6 Address:

::/0

Administrative Access

☒ HTTPS

☒ SSH

☒ PING

☒ SNMP

☐ HTTP

☐ TELNET

☐ FMG-Access

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ SSH

☐ PING

☐ SNMP

☐ HTTP

☐ TELNET

☐ FMG-Access

## Downloading the Fortinet MIB files to and configuring an example SNMP manager

Go to **System > Config > SNMP** to download FortiGate SNMP MIB file and the Fortinet Core MIB file.

Two types of MIB files are available for FortiGate units: the Fortinet MIB, and the FortiGate MIB. The Fortinet MIB contains traps, fields, and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields, and information that is specific to FortiGate units.

Configure the SNMP manager at 192.168.1.114 to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs.

## Results

This example uses the SolarWinds SNMP trap viewer.

In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.

SNMP Agent	<input checked="" type="checkbox"/> Enable
Description	Company FortiGate unit
Location	Head Office, server room
Contact	admin@company.com
<input type="button" value="Apply"/>	

### SNMP v1/v2c

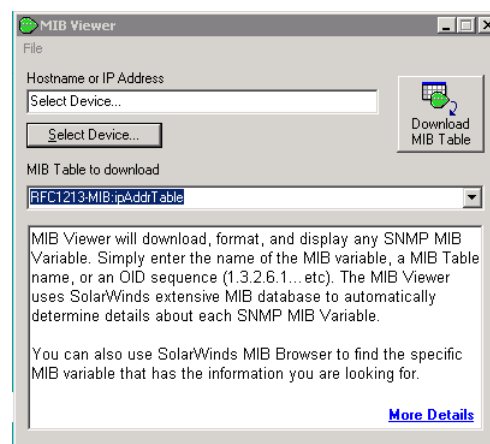
	Community Name	Queries	Traps	Enable
	FortiGates	✓	✓	<input checked="" type="checkbox"/>

### SNMP v3

	User Name	Security Level	Notification Host	Queries
--	-----------	----------------	-------------------	---------

### FortiGate SNMP MIB

[Download FortiGate MIB File](#)  
[Download Fortinet Core MIB File](#)



Open the SNMP Trap Receiver and select **Launch**.

**Device Credentials**

Device or IP address:

Credentials:

☒ Community string:

☐ SNMP Version 3:


1 search results for **SNMP Trap Receiver**

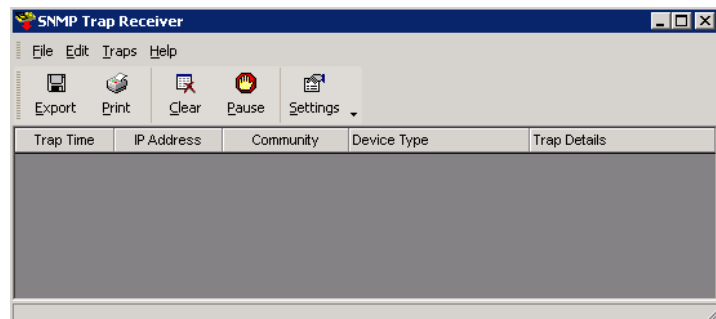
**SNMP Trap Receiver**

Logs, and display SNMP traps sent from a network device, server, or application

- Receives, logs, and displays SNMP traps
- Includes traps that are sent from a network device, server or application

Launch








On the FortiGate unit, perform an action to trigger a trap (for example, change the IP address of the DMZ interface).

Verify that the SNMP manager receives the trap.

On the FortiGate unit, view log messages showing the trap was sent by going to **Log & Report > Event Log > System**.

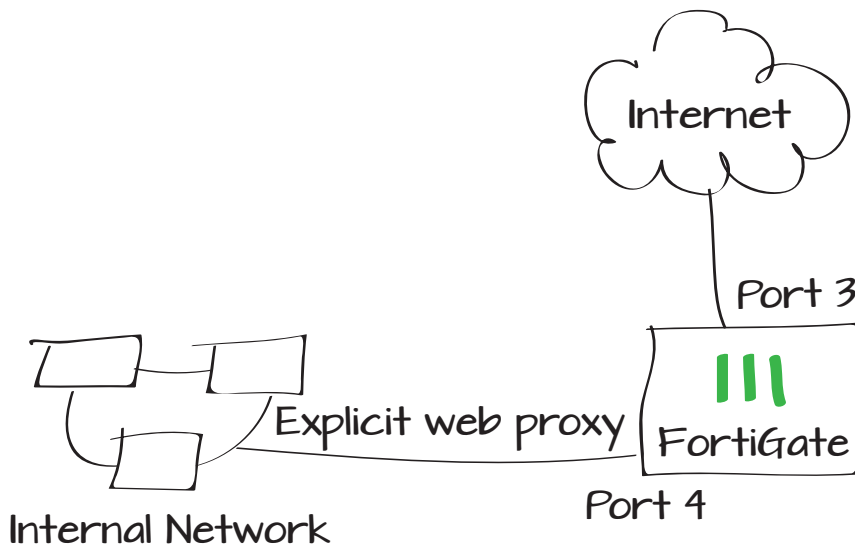
Trap Time	IP Address	Community	Device Type	Trap Details
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapInfg.1.3.0.201 fnTrapInfg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.201 fnTrapInfg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2 experimental.1057.1 = 192.168.1.99
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.6.0.1004 fnTrapInfg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.1004 fnTrapInfg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0 experimental.1057.1 = 192.168.1.99

cfgpath	system.interface	Date/Time	10:49:28 (Fri Mar 8 10:49:28 2013)
Virtual Domain	root	Level	information
Timestamp	Fri Mar 8 10:49:28 2013	cfgtid	2949201
logid	44547	Sub Type	system
User Interface	GUI(172.20.120.21)	User	 admin
Action	Edit	cfgobj	dmz
roll	65409	cfgattr	ip[10.10.10.99 255.255.255.0->10.10.10.1
Message	Edit system.interface dmz		

# Setting up an explicit proxy for users on a private network

In this example, an explicit web proxy is set to accommodate faster web browsing. This allows internal users to connect using port 8080 rather than port 80.

1. Enabling explicit web proxy on the internal interface
2. Configuring the explicit web proxy for HTTP/HTTPS traffic
3. Adding a security policy for proxy traffic
4. Results



# Enabling explicit web proxy on the internal interface

Go to **System > Network > Interfaces**.

Edit an internal port (port 4 in the example).  
**Enable** both **DHCP Server** and **Explicit Web Proxy**.

Go to **System > Config > Features**. Ensure that **WAN Opt. & Cache** is enabled.

Name

port4 (00:09:0F:4E:0E:C2)

Alias

Internal Interface

Link Status

Down

Type

Physical Interface

Addressing mode

Manual

DHCP

PPPoE

One-Arm Sniffer

Dedicate to

IP/Network Mask

10.10.1.99/255.255.255.0

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☐ FMG-Access

☒ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
10.10.1.100	10.10.1.200

Netmask

255.255.255.0

Default Gateway

Same as Interface IP

Specify

DNS Server

Same as System DNS

Specify

Advanced...

Security Mode

None

Device Management

Detect and Identify Devices

☐

Enable Explicit Web Proxy

☒

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

☐

Comments

Write a comment...

0/255

Administrative Status

Up

Down

## Basic Features

Advanced Routing

ON

IPv6

ON

IPv6

WAN Opt. & Cache

ON

WiFi Controller



ON

## Configuring the explicit web proxy for HTTP/HTTPS traffic

Go to **System > Network > Explicit Proxy** and enable the HTTP/HTTPS explicit web proxy.

Ensure that the **Default Firewall Policy Action** is set to **Deny**.

### ▼ Explicit Web Proxy Options

Enable Explicit Web Proxy	<input checked="" type="checkbox"/> HTTP / HTTPS <input type="checkbox"/> FTP <input type="checkbox"/> PAC
Listen on Interfaces	port4 
HTTP Port	<input type="text" value="8080"/>
HTTPS Port	<input type="text" value="0"/> (0 to use HTTP port)
FTP Port	<input type="text" value="0"/> (0 to use HTTP port)
PAC Port	<input type="text" value="0"/> (0 to use HTTP port)
PAC File Content	
Proxy FQDN	<input type="text" value="default.fqdn"/>
Max HTTP request length	<input type="text" value="4"/> Kb
Max HTTP message length	<input type="text" value="32"/> Kb
Unknown HTTP version	<input type="text" value="Best Effort"/>
Realm	<input type="text" value="default"/>
Default Firewall Policy Action	<input type="radio"/> Accept <input checked="" type="radio"/> Deny

# Adding a security policy for proxy traffic

Go to **Policy > Policy > Policy**.

Create a new policy and set the **Incoming Interface** to **web-proxy**, the **Outgoing Interface** to an internal port (in the example, port 3), and the **Service** to **webproxy**.

## Results

Configure web browsers on the private network to connect using a proxy server. The IP address of the HTTP proxy server is 10.10.1.99 (the IP address of the FortiGate internal interface) and the port is 8080 (the default explicit web proxy port). Web browsers configured to use the proxy server are able to connect to the Internet.

Go to **Policy > Policy > Policy** to see the ID of the policy allowing webproxy traffic.

Web proxy traffic is not counted by security policy.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Firewall

☐ VPN

☒ Address

☐ User Identity

☐ Device Identity

web-proxy

all

port3

all

always

webproxy

ACCEPT

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

☐ Web Proxy Forwarding Server

Click to set...

Security Profiles

OFF

AntiVirus

OFF

Web Filter

OFF

Application Control

OFF

IPS

OFF

DLP Sensor

OFF

SSL/SSH Inspection

default

default

default

default

default

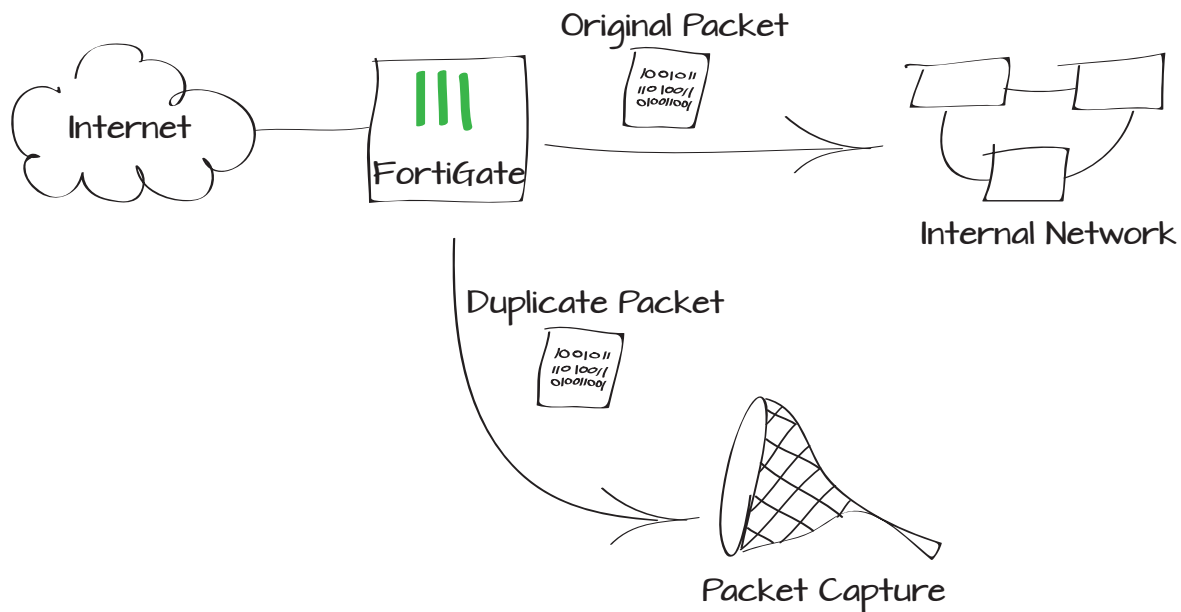
default

Create New Edit Delete					Section View Global View		
Seq.#	ID	Source	Destination	Service	Action	Log	Count
▶ port4 (Internal Interface) - port3 (External Interface) (1 - 2)							
▼ web-proxy - port3 (External Interface) (3 - 3)							
3	3	LAN	all	webproxy	ACCEPT	<input checked="" type="checkbox"/>	0 Packets / 0 B
▶ Implicit (4 - 4)							

# Adding packet capture to help troubleshooting

Packet capture is a means of logging traffic and its details to troubleshoot any issues you might encounter with traffic flow or connectivity. This example shows the basics of setting up packet capture on the FortiGate unit and analyzing the results.

1. Creating a packet capture filter
2. Starting the packet capture
3. Stopping the packet capture
4. Results



## Creating a packet capture filter

Go to **System > Network > Packet Capture**.

Create a new filter. In this example, the FortiGate unit will capture 100 HTTP packets on the internal interface from/to host 192.168.1.200.

- Host(s) can be a single IP or multiple IPs separated by comma, IP range, or subnet.
- Port(s) can be single or multiple separated by comma or range.
- Protocol can be single or multiple separated by comma or range. Use 6 for TCP, 17 for UDP, and 1 for ICMP.

Interface	internal
Max. Packets to Save	100
Capturing Progress	Not Running
0/100 Packets Captured	
<input checked="" type="checkbox"/> Enable Filters	
Host(s)	192.168.1.200
Port(s)	80
VLAN(s)	
Protocol	6
<input type="checkbox"/> Include IPv6 Packets	
<input type="checkbox"/> Include Non-IP Packets	

## Starting the packet capture

Select **Start** to begin the packet capture. Using an internal computer, or a device set to IP address 192.168.1.200, surf the Internet to generate traffic.

Interface	internal
Max. Packets to Save	100
Capturing Progress	
0/100 Packets Captured	
<input checked="" type="checkbox"/> Enable Filters	
Host(s)	192.168.1.200
Port(s)	80
VLAN(s)	
Protocol	6
<input type="checkbox"/> Include IPv6 Packets	
<input type="checkbox"/> Include Non-IP Packets	

## Stopping the packet capture

Once the FortiGate reaches the maximum number of packets to save (in this case 100), the capturing progress stops and you can download the saved pcap file.

You can also stop the capturing at any time before reaching the maximum number of packets.

## Results

Open the pcap file with a pcap file viewer, such as tcpdump or Wireshark.

Adjust the settings in the filter depending on the kind of traffic you wish to capture.

Go to **Log & Report > Event Log > System** to verify that the packet capture file downloaded successfully.




Interface

internal

Max. Packets to Save

100

Capturing Progress




100/100 Packets Captured

☒ Enable Filters


Host(s)

192.168.1.200




Port(s)

80




VLAN(s)



Protocol

6



☐ Include IPv6 Packets

☐ Include Non-IP Packets


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.200	173.194.77.94	TCP	66	64969 → http [SYN] Seq
2	0.045413	173.194.77.94	192.168.1.200	TCP	66	http → 64969 [SYN, ACK]
3	0.045683	192.168.1.200	173.194.77.94	TCP	60	64969 → http [ACK] Seq
4	0.045710	192.168.1.200	173.194.77.94	HTTP	761	GET /url?sa=&rcrt=ls&
5	0.086668	173.194.77.94	192.168.1.200	TCP	54	http → 64969 [ACK] Seq
6	0.093785	173.194.77.94	192.168.1.200	HTTP	625	HTTP/1.1 200 OK (text
7	0.203254	192.168.1.200	199.71.28.69	TCP	66	64970 → http [SYN] Seq
8	0.218907	199.71.28.69	192.168.1.200	TCP	66	http → 64970 [SYN, ACK]
9	0.219163	192.168.1.200	199.71.28.69	TCP	60	64970 → http [ACK] Seq
10	0.219185	192.168.1.200	199.71.28.69	HTTP	559	GET /eng/ HTTP/1.1
11	0.239078	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
12	0.239097	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
13	0.239345	192.168.1.200	199.71.28.69	TCP	60	64970 → http [ACK] Seq
14	0.258854	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
15	0.260813	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
16	0.260833	199.71.28.69	192.168.1.200	TCP	1434	[TCP segment of a reas
17	0.261260	192.168.1.200	199.71.28.69	TCP	60	64970 → http [ACK] Seq

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

- Ethernet II, Src: dell\_ea:6c:c6 (f0:ad:a2:ea:6c:c6), Dst: Fortinet\_99:39:70 (00:09:0f:99:00:30)
- Internet Protocol Version 4, Src: 192.168.1.200 (192.168.1.200), Dst: 173.194.77.94 (173.194.77.94)
- Transmission Control Protocol, Src Port: 64969 (64969), Dst Port: http (80), Seq: 0, Len: 0

```

0000  00 09 0f 99 39 70 f0 ad a2 ea 6c c6 00 08 40 45 00      ...9p.M...!..E.
0010  00 10 34 6c id 40 00 80 06 d1 15 c0 a8 01 c8 ad c2          .4l.0...
0020  4d se fd c9 00 00 2b 5e 97 9d 00 00 00 80 02         MA...P+H.....
0030  ff ff 0f 6f 00 02 04 05 b4 01 03 03 02 01 01        .....
0040  04 02
    
```

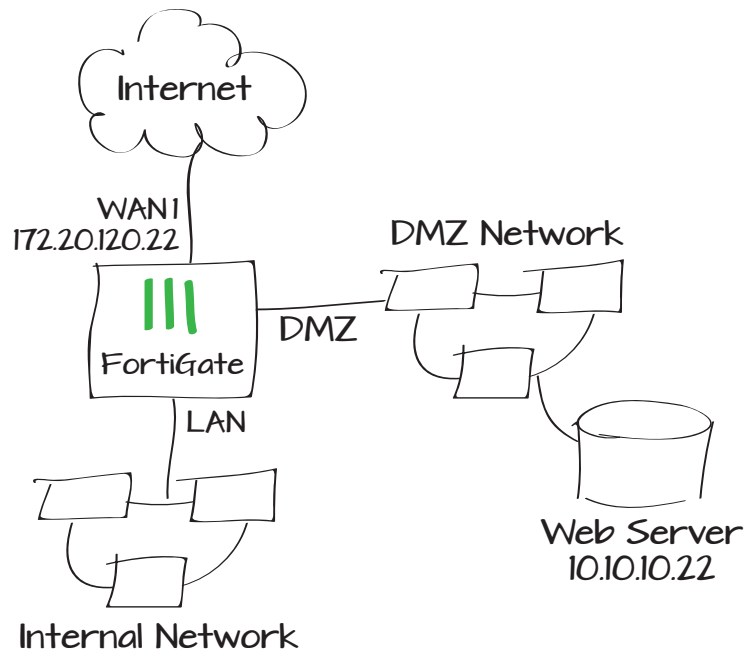
Status	success	Virtual Domain	root
Level	warning <div><div></div><div></div><div></div><div></div><div></div></div>	Timestamp	Thu Mar 21 11:55:20 2013
Log ID	32095	Sub Type	system
User Interface	GUI(172.20.120.21)	User	 admin
Action	download	Date/Time	11:55:20 (Thu Mar 21 11:55:20 2013)
roll	65535	Message	Packet Capture File file has been downloaded b



# Protecting a web server on the DMZ network

In the following example, a web server is connected to a DMZ network. An internal-to-DMZ security policy allows internal users to access the web server using an internal IP address (10.10.10.22). A WAN-to-DMZ security policy hides the internal address, allowing external users to access the web server using a public IP address (172.20.120.22).

1. Configuring the FortiGate unit's DMZ interface
2. Adding virtual IPs
3. Creating security policies
4. Results



# Configuring the FortiGate unit's DMZ interface

Go to **System > Network > Interfaces**.

Edit the **DMZ** interface. A DMZ Network (from the term 'demilitarized zone') is a secure network connected to the FortiGate that only grants access if it has been explicitly allowed. Using the DMZ interface is recommended but not required.

## Adding virtual IPs

Go to **Firewall Objects > Virtual IPs > Virtual IPs**.

Create two virtual IPs: one for HTTP access and one for HTTPS access.

Each virtual IP will have the same address, mapping from the public-facing interface to the DMZ interface. The difference is the port for each traffic type: port 80 for HTTP and port 443 for HTTPS.

Name

dmz (00:09:0f:4e:0e:ba)

Alias

DMZ server network

Link Status

Up

Type

Physical Interface

Addressing mode

☒ Manual ☐ DHCP ☐ PPPoE ☐ One-Arm Sniffer ☐

IP/Network Mask

10.10.10.1/255.255.255.0

Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access

☐ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

DHCP Server

☐ Enable

Security Mode

None

Device Management

Detect and Identify Devices

☐

Enable Explicit Web Proxy

☐

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

☐

Comments

Write a comment... 0/255

Administrative Status

☒ Up ☐ Down

Name

Web server http access

Comments

Write a comment... 0/255

Color

[Change]

External Interface

wan1

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

172.20.120.22 - 172.20.120.22

Mapped IP Address/Range

10.10.10.22 - 10.10.10.22

☒ Port Forwarding

Protocol

☒ TCP ☐ UDP ☐ SCTP

External Service Port

80 - 80

Map to Port

80 - 80

66

The FortiGate Cookbook 5.0.7

# Creating security policies

Go to **Policy > Policy > Policy**.

Create a security policy to allow HTTP and HTTPS traffic from the Internet to the DMZ interface and the web server.

Create a second security policy to allow HTTP and HTTPS traffic from the internal network to the DMZ interface and the web server.

Adding this policy allows traffic to pass directly from the internal interface to the DMZ interface.

Name	Web server https access	
Comments	Write a comment... 0/255	
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.22	- 172.20.120.22
Mapped IP Address/Range	10.10.10.22	- 10.10.10.22
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	443	- 443
Map to Port	443	- 443

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	wan1
Source Address	all
Outgoing Interface	dmz (DMZ server network)
Destination Address	Web server http access
	Web server https access
Schedule	always
Service	HTTP
	HTTPS
Action	ACCEPT

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	internal
Source Address	all
Outgoing Interface	dmz (DMZ server network)
Destination Address	all
Schedule	always
Service	HTTP
	HTTPS
Action	ACCEPT

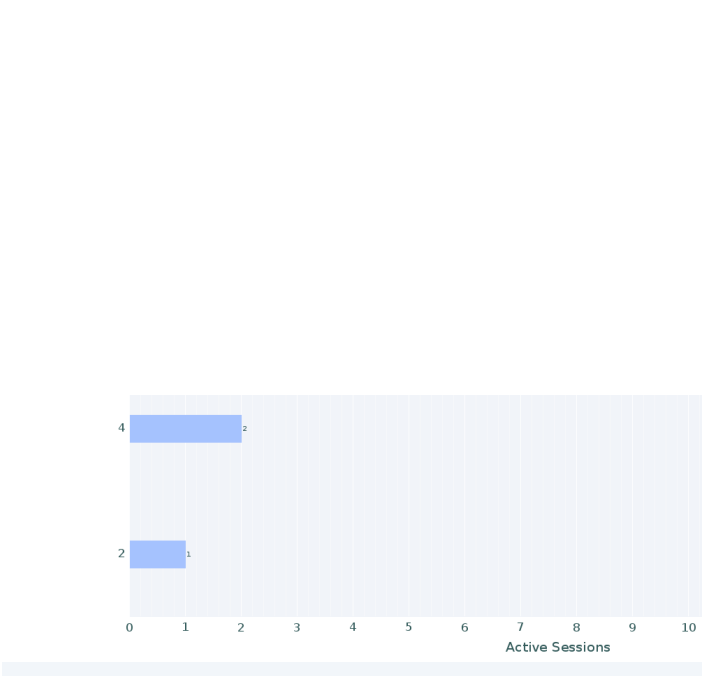
# Results

External users can access the web server on the DMZ network from the Internet using `http://172.20.120.22` and `https://172.20.120.22`.

Internal users can access the web server using `http://10.10.10.22` and `https://10.10.10.22`.

Go to **Policy > Monitor > Policy Monitor**.

Use the policy monitor to verify that traffic from the Internet and from the internal network is allowed to access the web server. This verifies that the policies are configured correctly.





Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
4	internal	dmz	✓	2	1.76 MB	2,943
2	wan1	dmz	✓	1	45.86 KB	315

Go to **Log & Report > Traffic Log > Forward Traffic**.

The traffic log shows sessions from the internal network and from the Internet accessing the web server on the DMZ network.

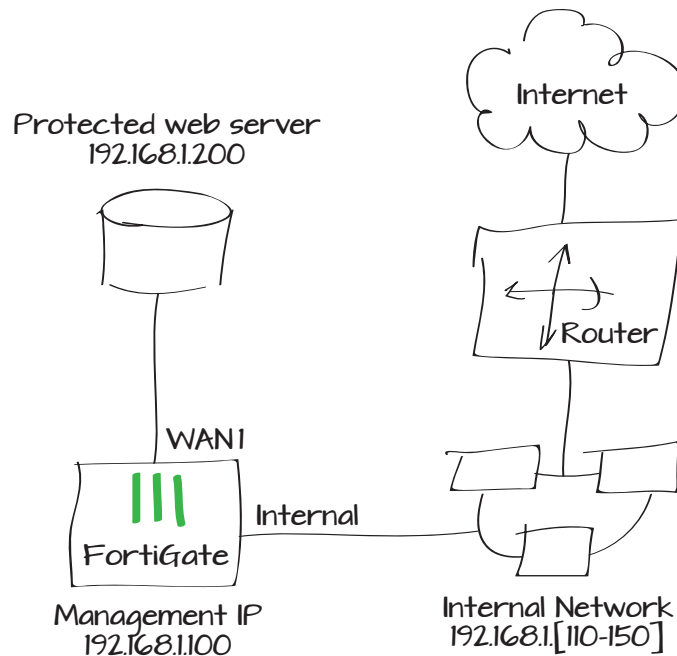
<div><div>Refresh</div><div>Download Raw Log</div></div>						
#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst	
3	3 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	48 B
4	3 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	0 B
5	4 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	0 B
6	31 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	1.21
7	31 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	1.16

<div><div> Refresh</div><div> Download Raw Log</div></div>					
#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	
▶ 1	4 seconds ago	wan1	dmz	172.20.120.21	172.20.120.22
2	57 seconds ago	wan1	dmz	172.20.120.123	172.20.120.22
3	1 minute ago	wan1	dmz	172.20.120.123	172.20.120.22

# Using port pairing to simplify transparent mode

When you create a port pair, all traffic accepted by one of the paired ports can only exit out the other port. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

1. Switching the FortiGate unit to transparent mode and adding a static route
2. Creating an internal and wan1 port pair
3. Creating firewall addresses
4. Creating security policies
5. Results



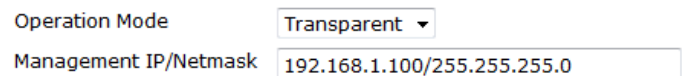
## Switching the FortiGate unit to transparent mode and adding a static route

Go to **System > Dashboard > Status**.

In the **System Information** widget, select **Change**. Set **Operation mode** to **Transparent**.

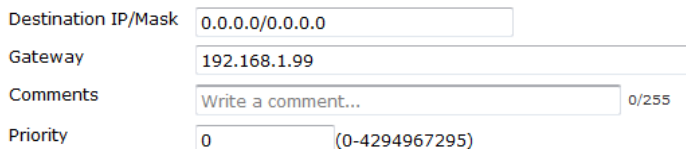
Log into the FortiGate unit using the management IP (in the example, 192.168.1.100).

Go to **System > Network > Routing Table** and set a static route.



Operation Mode: Transparent

Management IP/Netmask: 192.168.1.100/255.255.255.0



Destination IP/Mask: 0.0.0.0/0.0.0.0

Gateway: 192.168.1.99

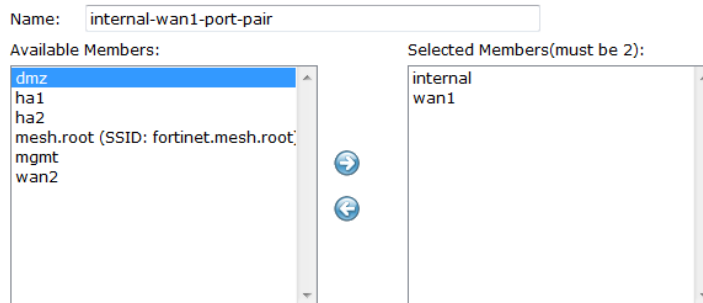
Comments: Write a comment... 0/255

Priority: 0 (0-4294967295)

## Creating an internal and wan1 port pair

Go to **System > Network > Interfaces**.

Create an internal/wan1 pair so that all traffic accepted by the internal interface can only exit out of the wan1 interface.



Name: internal-wan1-port-pair

Available Members:

- dmz
- ha1
- ha2
- mesh.root (SSID: fortinet.mesh.root)
- mgmt
- wan2

Selected Members(must be 2):

- internal
- wan1

# Creating firewall addresses

Go to **Firewall Objects > Address > Addresses**.

Create an address for the web server using the web server's Subnet IP.

Create a second address, with an IP range for internal users.

# Creating security policies

Go to **Policy > Policy > Policy**.

Create a security policy that allows internal users to access the web server using HTTP and HTTPS.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Web\_Server

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.200

Interface

Any

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal\_Users

Color

[Change]

Type

IP Range

Subnet / IP Range

192.168.1.110-192.168.1.150

Interface

Any

Show in Address List

☒

Comments

Write a comment... 0/255

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

Internal\_Users

Outgoing Interface

wan1

Destination Address

Web\_Server

Schedule

always

Service

HTTP HTTPS

Action

ACCEPT

Create a second security policy that allows connections from the web server to the internal users' network and to the Internet using any service.

## Results

Connect to the web server from the internal network and surf the Internet from the server itself.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that there is traffic from the internal to wan1 interface.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

wan1

Source Address

Web\_Server

Outgoing Interface

internal

Destination Address

all

Schedule

always

Service

ALL




Action

ACCEPT

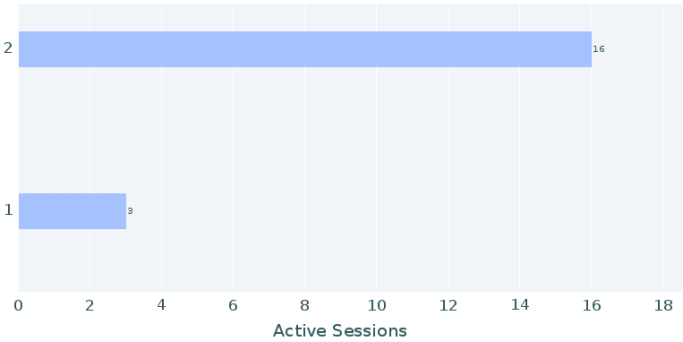
Src Interface	Dst Interface	Src	Dst	Sent / Received	Policy ID
wan1	internal	192.168.1.200	8.8.8.8	75 B / 286 B	2
wan1	internal	192.168.1.200	8.8.8.8	77 B / 277 B	2
wan1	internal	192.168.1.200	74.125.225.223	1.04 KB / 9.08 KB	2
wan1	internal	192.168.1.200	74.125.226.79	728 B / 2.62 KB	2
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
internal	wan1	192.168.1.111	192.168.1.200	1.46 KB / 2.92 KB	1
internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.70 KB	1
internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.75 KB	1
wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2
wan1	internal	192.168.1.200	74.125.226.67	58.06 KB / 2.06 MB	2



Select an entry for details.

Dst	 74.125.225.223	Virtual Domain	root
Received	9296	Source Country	Reserved
Application Name	 SSL	Sent / Received	1.04 KB / 9.08 KB
Duration	17	Sent	1067
Application Details		Service	HTTPS
Protocol	6	Destination Country	United States
Application Control List	default	Dst Port	443
roll	65531	Status	close
Timestamp	Wed Mar 13 11:05:11 2013	Tran Display	noop
Sequence Number	700150	Policy ID	2
Src Interface	wan1	Src	192.168.1.200
Sent Packets	15	Level	notice 
Application Category	Web.Surfing	Application ID	15895
Src Port	51218	Application Control Action	detected
Log ID	13	Sub Type	forward

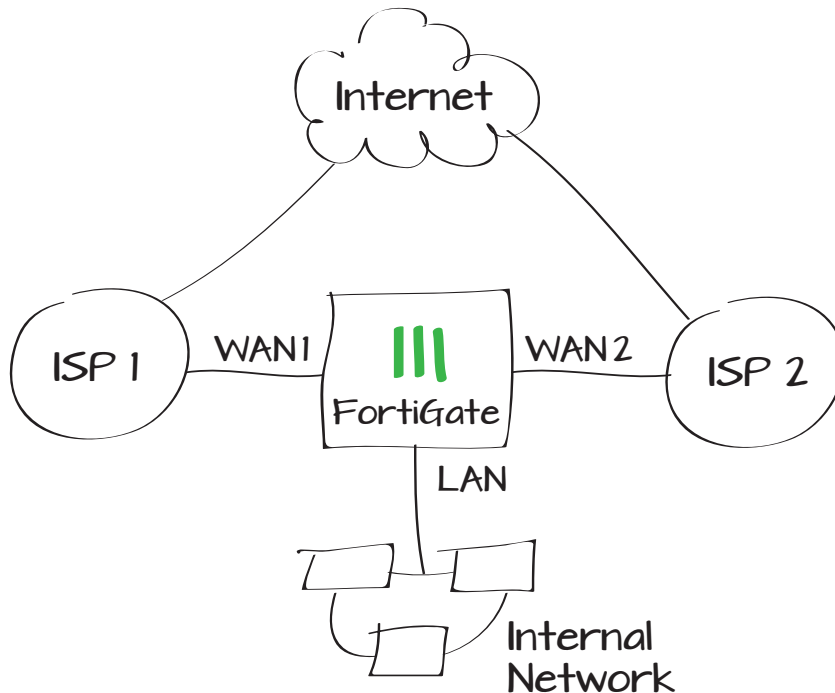
Go to **Policy > Monitor > Policy Monitor** to view the active sessions.



# Using two ISPs for redundant Internet connections

This example describes how to improve the reliability of a network connection using two ISPs. The example includes the configuration of equal cost multi-path load balancing, which efficiently distributes sessions to both Internet connections without overloading either connection.

1. Configuring connections to the two ISPs
2. Adding security policies
3. Configuring failover detection and spillover load balancing
4. Results



# Configuring connections to the two ISPs

Go to **System > Network > Interfaces** and configure the wan1 and wan2 connections. Make sure that both use **DHCP** as the **Addressing mode** and have **Retrieve default gateway from server** and **Override internal DNS** enabled.

Name

wan1 (00:09:0F:4E:0E:B9)

Alias

Link Status

Up

Addressing mode

☐ Manual

☒ DHCP

☐ Dedicate to FortiAP/FortiSwitch

Status:

connected

Obtained IP/Netmask:

120.20.120.223/255.255.255.0 

Renew

Expiry Date:

Mon Feb 11 12:14:55 2013

Acquired DNS:

192.168.110.9 204.187.144.34

Distance:

10

☒ Retrieve default gateway from server.

☒ Override internal DNS.

Administrative Access

☒ HTTPS

☐ PING

☒ HTTP

☐ FMG-Access

☒ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

Name

wan2 (00:09:0F:99:39:6C)

Alias

Link Status

Up

Addressing mode

☐ Manual

☒ DHCP

☐ One-Arm Sniffer

☐ Dedicate to FortiAP/F

Status:

connected

Obtained IP/Netmask:

172.20.120.226/255.255.255.0 

Renew

Expiry Date:

Fri Jan 11 08:36:03 2013

Acquired DNS:

192.168.110.9 204.187.144.34

Distance:

10

☒ Retrieve default gateway from server.

☒ Override internal DNS.

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☒ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

# Adding security policies

Go to **Policy > Policy > Policy**.

Create a security policy for the primary interface connecting to the ISPs and the internal network.

Create a security policy for each interface connecting to the ISPs and the internal network.

# Configuring failover detection and spillover load balancing

Go to **Router > Static > Settings**.

Create two new **Dead Gateway Detection** entries.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

all

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

all

Outgoing Interface

wan2

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Interface

wan1

Gateway IP

0.0.0.0

Ping Server

pingserver.fortinet.net

Detect Protocol

ICMP Ping

Ping Interval (seconds)

2

Failover Threshold (Pings lost consecutively)

2

HA Priority

1

Set the **Ping Interval** and **Failover Threshold** to a smaller value for a more immediate reaction to a connection going down.

Go to **Router > Static > Settings** and set the **ECMP Load Balancing Method** to **Spillover**.

The Spillover Threshold value is calculated in kbps (kilobits per second). However, the bandwidth on interfaces is calculated in kBps (kilo Bytes per second).

For wan1 interface, Spillover Threshold = 100 kbps = 100000 bps. Assume that 1000 bps is equal to 1024 bps. Thus, 100000 bps = 102400 bps = 102400/8 Bps = 12800 Bps.

## Results

Go to **Log & Report > Traffic Log > Forward Traffic** to see network traffic from different source IP addresses flowing through both wan1 and wan2.

Interface	wan2
Gateway IP	0.0.0.0
Ping Server	pingserver.fortinet.net
Detect Protocol	ICMP Ping
Ping Interval (seconds)	2
Failover Threshold (Pings lost consecutively)	2
HA Priority	1










### ECMP Load Balancing Method

☐ Source IP based ☐ Weighted Load Balance ☒ Spillover

Edit	
Interface	Spillover Threshold
dmz	0
ha1	0
ha2	0
internal	0
mesh.dmgmt-vdom	0
mesh.root	0
mgmt	0
modem	0
ssl.dmgmt-vdom	0
ssl.root	0
wan1	100
wan2	200

#	Y Date/Time	Y Src	Y Dst	Y Src Interface	Y Dst Interface	Y Sen
1	08:10:40	192.168.1.100	107.14.43.169	internal	wan2	820 B / 762 B
2	08:10:38	192.168.1.100	74.125.226.77	internal	wan2	585 B / 333 B
3	08:10:38	192.168.1.100	74.125.226.89	internal	wan1	840 B / 20.17 KB
4	08:10:38	192.168.1.111	69.25.24.24	internal	wan1	717 B / 1.48 KB
5	08:10:34	192.168.1.111	69.89.93.5	internal	wan1	1.83 KB / 5.83 KB
6	08:10:34	192.168.1.111	69.89.93.5	internal	wan1	1.33 KB / 5.19 KB
7	08:10:34	192.168.1.111	66.185.85.15	internal	wan1	16.46 KB / 1.00 M
8	08:10:34	192.168.1.111	66.185.85.15	internal	wan1	52.38 KB / 3.49 M
9	08:10:34	192.168.1.111	107.22.183.12	internal	wan2	1.90 KB / 2.47 KB

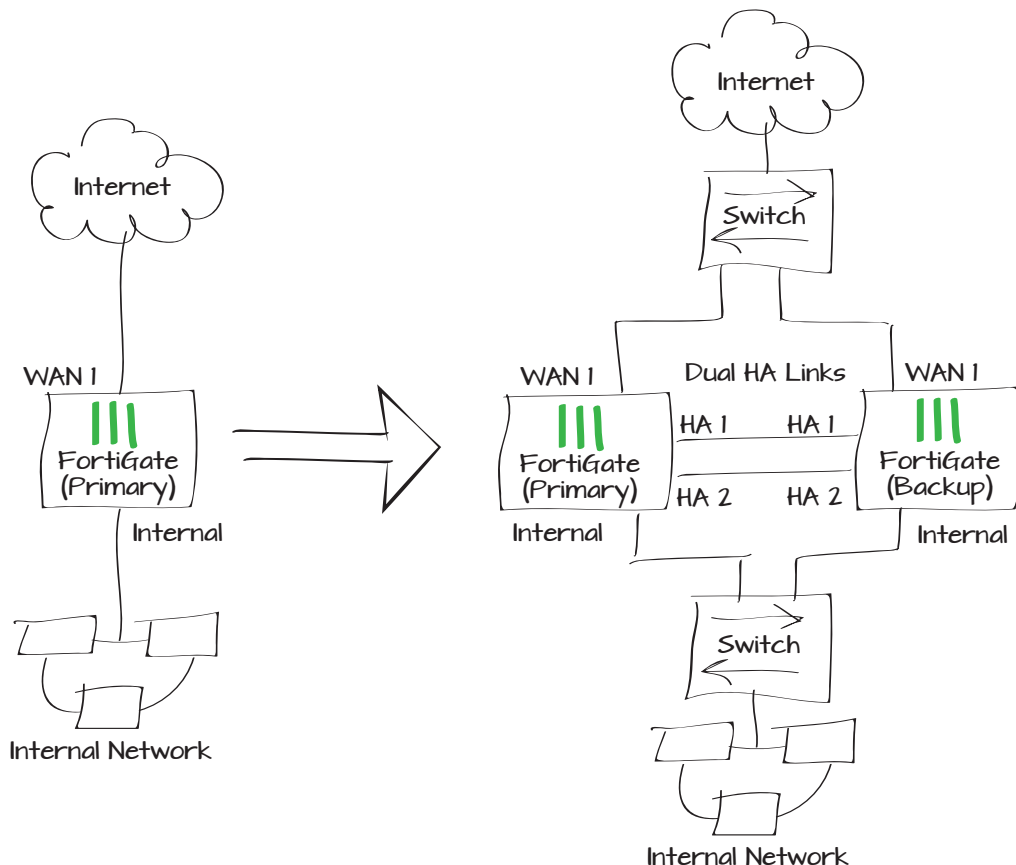
Disconnect the wan1 port on the FortiGate unit to see that all traffic automatically goes through the wan2 port unit, until wan1 is available again.

#	▼ Date/Time	▼ Src	▼ Dst	▼ Src Interface	▼ Dst Interface	▼ Sent
▶ 1	11:22:41	192.168.1.111	 74.125.226.15	internal	wan2	168 B / 88 B
2	11:22:41	192.168.1.111	 50.18.91.127	internal	wan2	730 B / 682 B
3	11:22:41	192.168.1.111	 107.6.106.10	internal	wan2	3.02 KB / 5.89 K
4	11:22:38	192.168.1.111	 68.67.159.216	internal	wan2	853 B / 1.18 KB
5	11:22:37	192.168.1.111	 68.67.159.216	internal	wan2	860 B / 1.06 KB
6	11:22:37	192.168.1.111	 68.67.159.216	internal	wan2	912 B / 896 B
7	11:22:34	192.168.1.111	 72.21.91.113	internal	wan2	1.19 KB / 9.12 K
8	11:22:34	192.168.1.111	 74.125.226.4	internal	wan2	168 B / 88 B
9	11:22:24	192.168.1.111	 72.21.91.113	internal	wan2	1.69 KB / 18.18

# Adding a backup FortiGate unit to improve reliability

Adding a backup FortiGate unit to a currently installed FortiGate unit provides redundancy if the primary FortiGate unit fails. This system design is known as High Availability (HA) and is intended to improve network reliability.

1. Adding the backup FortiGate unit and configuring HA
2. Testing the failover functionality
3. Upgrading the firmware for the HA cluster



# Adding the backup FortiGate unit and configuring HA

Connect the backup FortiGate unit as shown in the diagram.

Go to **System > Dashboard > Status**.

Change the host name of the primary FortiGate unit.

Go to **System > Config > HA**.

Configure the HA settings for the primary FortiGate unit.

**Current Name** FG100D3G12804195

**New Name**

Mode

Device Priority

☐ Reserve Management Port for Cluster Member

## Cluster Settings

Group Name

Password

☒ Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
ha1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
ha2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
internal		<input type="checkbox"/>	<input type="text" value="0"/>
mgmt	<input type="checkbox"/>		
wan1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
wan2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

**Current Name** FG100D3G12804195

**New Name**

Go to **System > Dashboard > Status**.

Change the host name of the backup FortiGate unit.



Go to **System > Config > HA**.

Configure the HA settings for the backup FortiGate unit.

Ensure that the **Group Name** and **Password** are the same as on the primary FortiGate unit.

Go to **System > Config > HA** to view the cluster information.

Select **View HA Statistics** for more information on the cluster.

Mode

Active-Passive

Device Priority

128

☐ Reserve Management Port for Cluster Member

WLAN\_1 (SSID: FortiDocs1)

Cluster Settings

Group Name


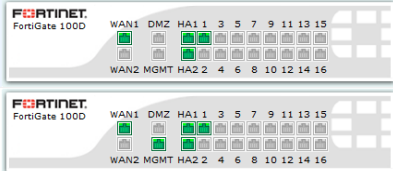

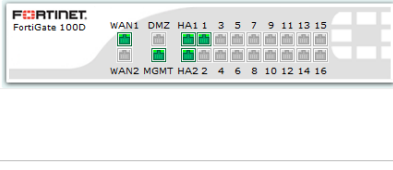
FGT-HA



Password

.....

☒ Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<div>0</div>
ha1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<div>50</div>
ha2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<div>50</div>
internal	<input type="checkbox"/>	<input type="checkbox"/>	<div>0</div>
mgmt	<input type="checkbox"/>	<input type="checkbox"/>	<div></div>
wan1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div>0</div>
wan2	<input type="checkbox"/>	<input type="checkbox"/>	<div>0</div>

	Cluster Member	Hostname	Serial No.	Role
		Primary_FGT	FG100D3G12801361	MASTER
		Backup_FGT	FG100D3G12802485	SLAVE

Unit	Status	Up Time	Monitor	
Primary_FGT FG100D3G12801361		0 days	CPU Usage	Active Sessions
		23 hours	<div>0%</div>	13
		3 minutes	Memory Usage	Network Utilization
		6 seconds	<div>41%</div>	0 Kbps
				Total Bytes
Backup_FGT FG100D3G12802485		0 days	CPU Usage	Active Sessions
		2 hours	<div>0%</div>	6
		24 minutes	Memory Usage	Network Utilization
		14 seconds	<div>31%</div>	0 Kbps
				Total Bytes

Go to **System > Dashboard > Status** to see the cluster information.

## Testing the failover functionality

Unplug the Ethernet cable from the WAN1 interface of the primary FortiGate unit. Traffic will divert to the backup FortiGate unit.

Use the **ping** command to view the results.

Shut down the primary FortiGate unit, and you will see that traffic fails over to the backup FortiGate unit.

Use the **ping** command to view the results.

System Information	
Cluster Name	FGT-HA
Cluster Members	Primary_FGT/FG100D3G12801361 Backup_FGT/FG100D3G12802485
Serial Number	FG100D3G12801361
Operation Mode	NAT [Change]
HA Status	Active-Passive [Configure]
System Time	Wed Nov 21 13:45:56 2012 (FortiGuard) [Change]
Firmware Version	v5.0,build0128 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /3 in Total [Details]
Uptime	0 day(s) 23 hour(s) 3 min(s)
Virtual Domain	Disabled [Enable]

```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

```
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 192.168.1.99: Destination net unreachable.
Reply from 192.168.1.99: Destination net unreachable.
Reply from 192.168.1.99: Destination net unreachable.
Request timed out.
Reply from 8.8.8.8: bytes=32 time=104ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
```

# Upgrading the firmware for the HA cluster

When a new version of the FortiOS firmware becomes available, upgrade the firmware on the primary FortiGate unit and the backup FortiGate unit will upgrade automatically.

Go to **System > Dashboard > Status** and view the **System Information** widget. Select **Upgrade** beside the **Firmware Version** listing.

The firmware will load on the primary FortiGate unit, and then on the backup unit.

Go to **Log & Report > Event Log > System**.

Go to **System > Dashboard > Status**. View the **System Information** widget again. Both FortiGate units should have the new firmware installed.

System Information

Cluster Name	FGT-HA		
Cluster Members	Primary_FGT/FG100D3G12801361 (Master)		
	Backup_FGT/FG100D3G12802485 (Slave)		
Serial Number	FG100D3G12801361		
Operation Mode	NAT [Change]		
HA Status	Active-Passive [Configure]		
System Time	Wed Nov 21 14:18:58 2012 (FortiGuard) [Change]		
Firmware Version	v5.0,build0134 (Interim) [Update] [Details]		
System Configuration	[Backup] [Restore] [Revisions]		
Current Administrator	admin [Change Password] /1 in Total [Details]		
Uptime	0 day(s) 0 hour(s) 15 min(s)		
Virtual Domain	Disabled [Enable]		

Upgrade From

Local Hard Disk

Upgrade File

C:\FGT\_100D-v500-build0134-FORTINET.out

Browse...

Upgrade Partition

#2

Boot the New Firmware

☒

Format Boot Device First

☐

#	Date/Time	Level	User	Message
1	16 minutes ago	OK		HA activity report
2	21 minutes ago	OK		Link monitor: Interface ha2 was turned on
3	21 minutes ago	OK		Link monitor: Interface ha1 was turned on
4	24 minutes ago	OK	admin	User admin restored the image from GUI
5	24 minutes ago	OK	admin	User admin loaded an image from GUI

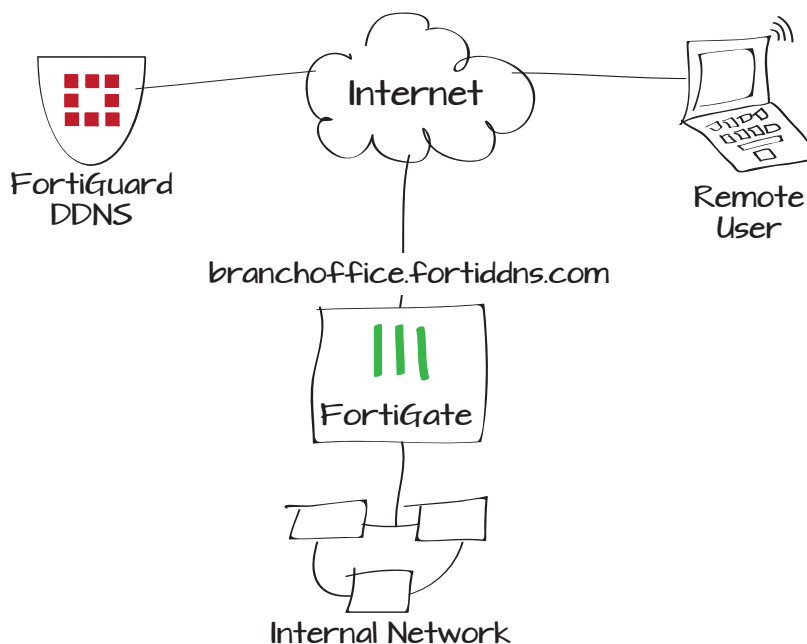
# Associating a domain name with an interface that has a dynamic IP

Using a Dynamic Domain Name Service (DDNS) means that users can reach your network by means of a domain name that remains constant even when its IP address changes. This example shows how to set up a FortiGate unit's Internet-facing interface to work with the FortiGuard DDNS.



The FortiGuard DDNS service requires an active FortiCare Support Contract.

1. Setting up FortiGuard DDNS from the GUI
2. Setting up FortiGuard DDNS from the CLI
3. Results



## Setting up FortiGuard DDNS from the GUI

Go to **System > Network > DNS** and enable FortiGuard DDNS.

Select the FortiGate **Interface** connected to the Internet, select a **Server**, and add a name for the network.

The FortiGuard DDNS service verifies that the resulting Domain name is unique and valid. The **Domain** name is then displayed with the current IP address of the interface. You can click the domain name to browse to the address with a web server.

## Setting up FortiGuard DDNS from the CLI

Go to **System > Dashboard > Status** and use the **CLI Console** to setup FortiGuard DDNS.

## Results

You can verify that the DDNS is working with a utility like dig or nslookup to check that the domain name resolves to the correct IP address.

### ☒ Enable FortiGuard DDNS

Interface	wan1
Server	fortiddns.com
Unique Location	branchoffice
Domain	branchoffice.fortiddns.com (172.20.120.126)

```
config system ddns
  edit 0
    set ddns-server FortiGuardDDNS
    set ddns-domain "branchoffice"
    set monitor-interface wan1
  end
```

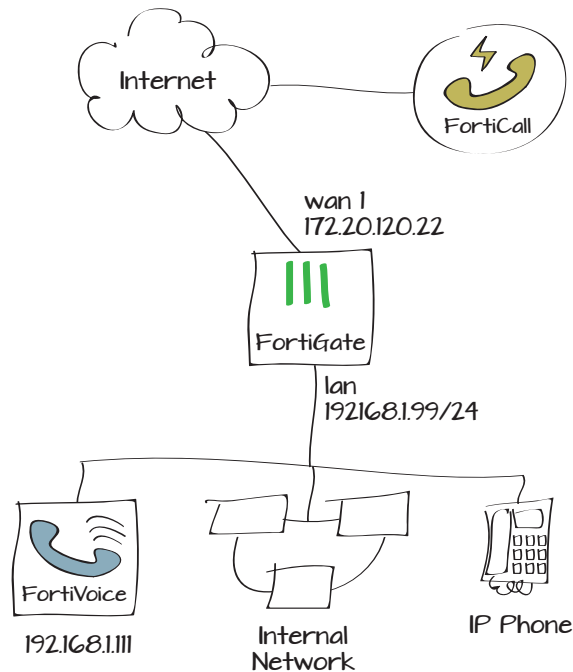
```
nslookup branchoffice.fortiddns.com
Server:      208.91.112.53
Address:     208.91.112.53#53

Non-authoritative answer:
Name: branchoffice.fortiddns.com
Address: 172.20.120.126
```

# Allowing VoIP calls using FortiVoice and FortiCall

This example sets up inbound and outbound Voice over IP (VoIP) calls using Session Initiation Protocol (SIP) through the FortiGate unit, using a FortiVoice unit and FortiCall services.

1. Setting up a FortiCall account
2. Configuring the FortiVoice unit
3. Configuring the FortiGate unit for outbound SIP calls
4. Configuring the FortiGate unit for inbound SIP calls
5. Results



## Setting up a FortiCall account

Go to [www.forticall.com](http://www.forticall.com) and follow the set up instructions. When the account is set up, you will be provided with information to activate your account. You will also need to choose a phone number for inbound calls.

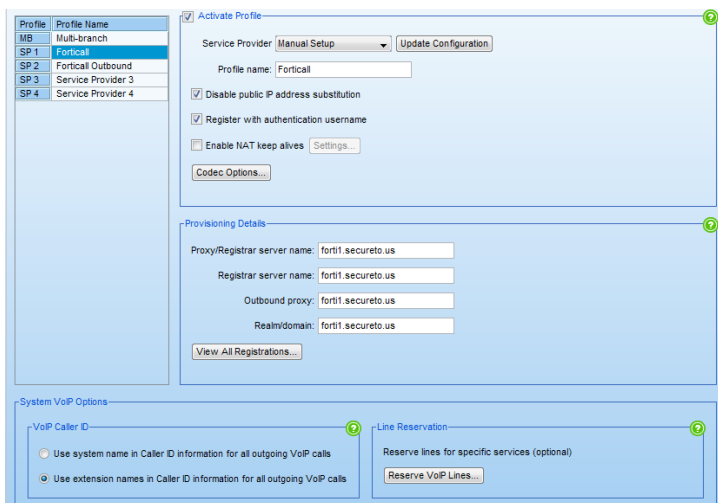
## Configuring the FortiVoice unit

Insert the CD into the CD-ROM drive, the FortiVoice Install main window will appear within 20 seconds. Click Install FortiVoice and follow the instructions.



Open the FortiVoice Management software

Go to **Global Settings > VoIP Configuration** and set up a service provider profile for inbound calls.



Set a service provider for outbound calls.

Profile	Profile Name
MB	Multi-branch
SP 1	Forticall
SP 2	Forticall Outbound
SP 3	Service Provider 3
SP 4	Service Provider 4

Activate Profile

Service Provider: Manual Setup Update Configuration

Profile name: Forticall Outbound

☒ Disable public IP address substitution

☐ Register with authentication username

☐ Enable NAT keep alives Settings...

Codec Options...

Provisioning Details

Proxy/Registrar server name: fort11.secureto.us

Registrar server name:

Outbound proxy:

Realm/domain:

View All Registrations...

Go to **Lines and Greetings > VoIP Numbers** and set your phone number for inbound calls.

ID	VoIP Number
1	1-343-8821592
2	1-613-8821592
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	

Activate VoIP Number

Select a VoIP Profile: Forticall

Phone Number

Country code: 1

City or area code: 343

Number: 8821592

User name and Password

User/Account: 000F4D003EBC

Password: Password

Registration Status

Status: Registered View All Registrations...

Call Handling

Mode 1 (Mode 1) Mode 2 (Mode 2) Holiday Mode (Holiday Mode)

When a call comes in on this phone number, perform the following action:

ring extensions Edit...

If all extensions are busy or the call is not answered:

perform no action after 5 rings.

Set a phone number for outbound calls.

ID	VoIP Number
1	1-343-8821592
2	1-613-8821592
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	

Activate VoIP Number

Select a VoIP Profile: Forticall Outbound

Phone Number

Country code: 1

City or area code: 613

Number: 8821592

User name and Password

User/Account:

Password:

Registration Status

Status: Unregistered View All Registrations...

Call Handling

Mode 1 (Mode 1) Mode 2 (Mode 2) Holiday Mode (Holiday Mode)

When a call comes in on this phone number, perform the following action:

go to voicemail 111



# Configuring the FortiGate unit for outbound SIP calls

Go to **Security Profiles > VoIP > Profiles**.

Create a new profile and set the **Limit REGISTER request** and **Limit INVITE request**.

Name	SIP	
Comments	Write a comment... 0/255	
<b>SIP</b>		
Limit REGISTER request	10	(requests/sec/policy)
Limit INVITE request	10	(requests/sec/policy)
<b>SCCP</b>		
Limit Call Setup	0	(Calls/min/client)

Go to **Firewall Objects > Address > Address**

Create an IP range for SIP phones.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address	
Name	Internal-SIP-Phones	
Color	[Change]	
Type	IP Range	
Subnet / IP Range	192.168.1.110-192.168.1.150	
Interface	lan	
Show in Address List	<input checked="" type="checkbox"/>	
Comments	Write a comment... 0/255	

Go to **Policy > Policy > Policy**.

Create a policy allowing outbound SIP traffic. Set **Incoming Interface** to LAN, **Source Address** to the new firewall address, and **Outgoing Interface** to your Internet-facing interface.

Under **Security Profiles**, enable **VoIP** and set it to use the new profile.

Make sure you place this security policy on the top of the policy list.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

☒ Log Allowed Traffic

Firewall

VPN

Address

User Identity

Device Identity

lan

Internal-SIP-Phones

wan1

all

always

SIP

ACCEPT

☒ Use Destination Interface Address

☐ Fixed Port

Click to add...

Security Profiles

OFF

Antivirus

OFF

Web Filter

OFF

Application Control

OFF

IPS

OFF

Email Filter

OFF

DLP Sensor

ON

VoIP

OFF

ICAP

OFF

SSL/SSH Inspection

default

default

default

default

default

default

SIP

default

default

Seq.#	ID	Source	Destination	Schedule
lan - wan1 (1 - 2)				
1	2	Internal-SIP-Phones	all	always
2	1	all	all	always

# Configuring the FortiGate unit for inbound SIP calls

Go to **Firewall Objects > Virtual IPs > Virtual IPs**

Create a new virtual IP mapping the external IP on the **wan1** interface of the FortiGate to the internal IP of the FortiVoice on UDP port 5060.

Go to **Policy > Policy > Policy**.

Create a policy allowing inbound SIP traffic. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to LAN, and **Destination Address** to the new virtual IP.

Enable **VoIP** and set it to use the new profile.

Name

Inbound\_SIP

Comments

Write a comment...

0/255

Color

[Change]

External Interface

wan1

Type

Static NAT

☐ Source Address Filter

(e.g.: x.x.x.x, x.x.x.x-y.y.y, x.x

External IP Address/Range

172.20.120.22

-

172.20.120.22

Mapped IP Address/Range

192.168.1.111

-

192.168.1.111

☒ Port Forwarding

Protocol

☐ TCP

☒ UDP

☐ SCTP

External Service Port

5060

-

5060

Map to Port

5060

-

5060

Policy Type

☒ Firewall

☐ VPN

Policy Subtype

☒ Address

☐ User Identity

☐ Device Identity

Incoming Interface

wan1

Source Address

all

Outgoing Interface

lan

Destination Address

Inbound\_SIP

Schedule

always

Service

SIP

Action

ACCEPT

☐ Enable NAT

☒ Log Allowed Traffic

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

OFF

IPS

default

OFF

Email Filter

default

OFF

DLP Sensor

default

ON

VoIP

SIP

OFF

ICAP

default

OFF

SSL/SSH Inspection

default

# Results







Go to **System > Dashboard > Status** and add the **VoIP Usage** widget.


When the widget appears, verify **Voice Calls**.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that both inbound and outbound SIP traffic is occurring.

Select an entry for details.

	SIP	SCCP
<b>Voice Calls</b>		
Currently Active Calls	0	0
Total Calls (since last reset)	5	0
Calls Failed/Dropped/Unanswered	0	0
Calls Succeeded	5	0

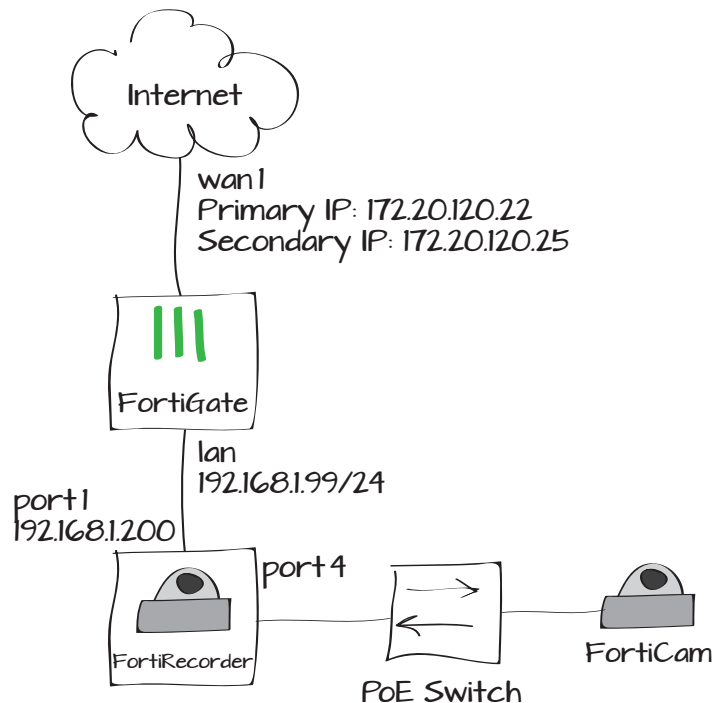
▼ Dst	▼ Sent / Received	▼ Policy ID	▼
172.20.120.22	574 B / 787 B	3	SIP
 66.11.10.43	14.79 KB / 20.84 KB	2	SIP
172.20.120.22	44.65 KB / 34.70 KB	3	SIP
172.20.120.22	40.69 KB / 31.42 KB	3	SIP
 66.11.10.43	110.16 KB / 107.42 KB	3	SIP
172.20.120.22	2.20 KB / 1.70 KB	3	SIP
 66.11.10.43	15.10 KB / 19.15 KB	2	SIP
 66.11.10.43	205.27 KB / 201.37 KB	2	SIP
172.20.120.22	4.64 KB / 3.97 KB	3	SIP
172.20.120.22	6.29 KB / 5.34 KB	3	SIP
 66.11.10.43	215.43 KB / 215.04 KB	3	SIP
 66.11.10.43	1.37 MB / 1.77 MB	2	SIP

Dst	172.20.120.22	Virtual Domain	root
Received	787	Source Country	United States
Sent / Received	574 B / 787 B	Dst NAT Port	5060
Duration	29	Sent	574
Application Details		Service	SIP
Protocol	17	Destination Country	Reserved
Dst Port	5060	roll	65530
Status	✓	Timestamp	Wed Jan 30 11:52:03 2013
Tran Display	dnat	Sequence Number	11819
Policy ID	3	Src Interface	wan1
Src	66.11.10.43	Dst NAT IP	192.168.1.111
Sent Packets	1	Level	notice 
Src Port	5060	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:52:03 (Wed Jan 30 11:52:03 2013)
Dst Interface	lan		

# Allowing access from the Internet to a FortiCamera unit

This example sets up a FortiRecorder unit and FortiCamera unit for use with a FortiGate unit. It also allows the FortiCamera unit, which is located on the internal network, to be accessed from the Internet

1. Configuring the FortiRecorder and FortiCamera units
2. Configuring the FortiGate unit's interfaces
3. Adding virtual IPs
4. Adding a security policy to allow access to the FortiCamera
5. Results



# Configuring the FortiRecorder and FortiCamera units

Connect locally to the FortiRecorder.

Go to **System > Network > Interface**.

Set an IP address for port1.

System

Configuration

Customization

Network

Administrator

Authentication

Certificate

Camera

Logs and Alerts

Edit Interface

Interface name: port1 (90:2b:34:58:1d:38)

☐ Discover cameras on this port

Addressing Mode

☒ Manual

IP/Netmask: 192.168.1.200 / 24

IPv6/Netmask: :: / 0

☐ DHCP

☐ Retrieve default gateway and DNS from server

☐ Connect to server

Access

☒ HTTPS ☒ PING ☐ HTTP

☒ SSH ☐ SNMP ☐ TELNET

☐ Override default MTU value (1500)

1500 (bytes)

Administrative status

☒ Up ☐ Down

Set an IP address for port4.

System

Configuration

Customization

Network

Administrator

Authentication

Certificate

Camera

Logs and Alerts

Edit Interface

Interface name: port4 (90:2b:34:58:1d:3b)

☒ Discover cameras on this port

Addressing Mode

☒ Manual

IP/Netmask: 192.168.200.2 / 24

IPv6/Netmask: :: / 0

☐ DHCP

☐ Retrieve default gateway and DNS from server

☐ Connect to server

Access

☐ HTTPS ☐ PING ☐ HTTP

☐ SSH ☐ SNMP ☐ TELNET

☐ Override default MTU value (1500)

1500 (bytes)

Administrative status

☐ Up ☒ Down

Go to **System > Network > DHCP**.

Create a DHCP server on port4 to lease IPs to FortiCamera.

The screenshot shows the FortiNet configuration interface with the 'DHCP' tab selected under the 'Network' section. The 'Network Interface Setting' section is expanded, showing the following configuration:

- ID: 1
- Enable DHCP server: ☒
- Interface: port4
- Gateway: 192.168.200.2
- DNS options: Default
- DNS server 1: 0.0.0.0
- DNS server 2: 0.0.0.0
- Domain:
- Netmask: 255.255.255.0

The 'Auto Config Setting' section is also expanded, showing:

- Lease time (Seconds): 604800
- Conflicted IP timeout (Seconds): 1800

The 'DHCP IP Range' section is expanded, showing a table with the following data:

Start	End
192.168.200.100	192.168.200.200

Below the table, there are checkboxes for 'DHCP Excluded IP Range' and 'Reserved IP Address', both of which are currently unchecked.

Go to **System > Network > Routing**.

Add a default route.

The screenshot shows the FortiNet configuration interface with the 'Routing' tab selected under the 'Network' section. The 'Edit Routing Entry' dialog is open, showing the following configuration:

- Destination IP/netmask: 0.0.0.0 / 0
- Gateway: 192.168.1.99

There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

Go to **Camera > Configuration > Camera**.

Click on **Force Discover** to have connected cameras displayed.

The screenshot shows the FortiNet configuration interface with the 'Camera' tab selected under the 'Configuration' section. The 'Camera' configuration page is displayed, showing a table of connected cameras. The table has the following columns: 'Enabled', 'Camera Name', 'Model', 'Location', and 'Address'. The first row shows a camera named 'Demo-Cam1-North' with model 'FCM-20A' and address '192.168.200.51'. The 'Force Discover' button is visible at the top right of the page.

# Configuring the FortiGate unit's interfaces

Go to **System > Network > Interfaces**.

Configure your Internet-facing interface. Select **Secondary IP Address** and create a new IP/Network Mask for the interface.

Adding a secondary IP address adds multiple IP addresses to the interface. The FortiGate unit, static and dynamic routing, and the network see the secondary IP addresses as additional IP addresses that terminate at the interface.

Configure the **lan** interface. Enable **DHCP Server** and create a new IP range.

Name

wan1(00:09:0F:99:39:6A)

Alias

Link Status

Up

Type

Physical Interface

Addressing mode

☒ Manual ☐ DHCP ☐ PPPoE ☐ Dedicate to FortiAP/FortiSwitch

IP/Network Mask

172.20.120.22/255.255.255.0

IPv6 Address

:::0

Administrative Access

☒ HTTPS ☒ PING ☒ HTTP ☐ FMG-Access ☒ CAPWAP  
☒ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ TELNET

DHCP Server

☐ Enable

Security Mode

None

Device Management

☐ Detect and Identify Devices

Enable Explicit Web Proxy

☐

Listen for RADIUS Accounting Messages

☐

Secondary IP Address

Create New

IP/Network Mask

Administrative Access

172.20.120.25/255.255.255.0

Name

lan

Type

Hardware Switch

Physical Interface Members

port1

X

port3

X

port4

X

port5

X

port6

X

port7

X

port8

X

port9

X

port10

X

port11

X

port12

X

port13

X

port14

X

port15

X

port16

X

port2

X

Addressing mode

☒ Manual ☐ DHCP ☐ PPPoE

IP/Network Mask

192.168.1.99/255.255.255.0

IPv6 Address

:::0

Administrative Access

☒ HTTPS ☒ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☒ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP  
☐ SSH ☐ SNMP ☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New

Starting IP

End IP

192.168.1.100

192.168.1.254

Netmask

255.255.255.0



# Adding virtual IPs

Go to **Firewall Objects >Virtual IPs > Virtual IPs.**

Create the two virtual IPs: one for HTTPS traffic and one for RTSP traffic. For both virtual IPs, set **External IP Address/Range** to the secondary IP of the Internet-facing interface and the **Mapped IP Address/Range** to the IP of port1 on the FortiRecorder unit.

# Adding a security policy

Go to **Policy > Policy > Policy.**

Create a policy allowing access to the FortiRecorder from the Internet. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to lan, and **Destination Address** to the new virtual IPs.

Name

FortiRecorder\_https

Comments

Write a comment...0/255

Color

[Change]

External Interface

wan1

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

172.20.120.25 - 172.20.120.25

Mapped IP Address/Range

192.168.1.200 - 192.168.1.200

☒ Port Forwarding

Protocol

☒ TCP ☐ UDP ☐ SCTP

External Service Port

443 - 443

Map to Port

443 - 443

Name

FortiRecorder\_rtsp

Comments

Write a comment...0/255

Color

[Change]

External Interface

wan1

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

172.20.120.25 - 172.20.120.25

Mapped IP Address/Range

192.168.1.200 - 192.168.1.200

☒ Port Forwarding

Protocol

☒ TCP ☐ UDP ☐ SCTP

External Service Port

554 - 554

Map to Port

554 - 554

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

wan1

Source Address

all

Outgoing Interface

lan

Destination Address

FortiRecorder\_https FortiRecorder\_rtsp

Schedule

always

Service

HTTPS RTSP

Action

ACCEPT

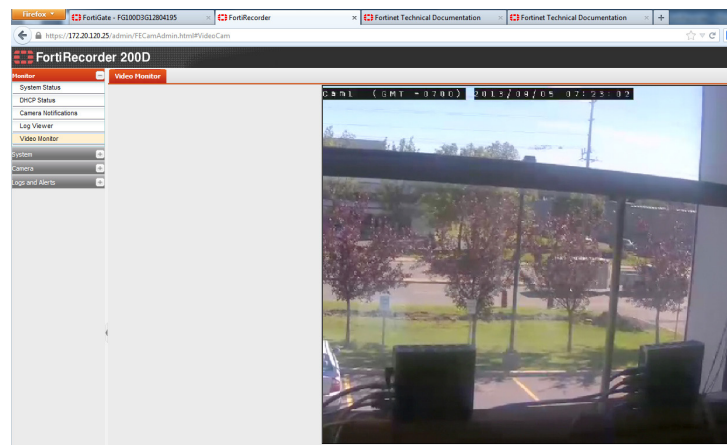
# Results

From the Internet, go to the IP address of the FortiGate unit's secondary IP (in the example, https://172.20.120.25) and you should be able to see securely live video feed using HTTPS and RTSP (Real Time Streaming Protocol)

Go to **Log & Report > Traffic > Forward Traffic**.

Verify https and RTSP traffic trough the FortiGate

Select an entry for details.



	▼ Dst	▼ Src Interface	▼ Dst Interface	▼ Service
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	RTSP
	172.20.120.21	lan	wan1	RTSP
	172.20.120.25	wan1	lan	RTSP
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS
	172.20.120.25	wan1	lan	HTTPS

Application Details		Date/Time	10:28:03 (1378376883)
Destination Country	Reserved	Dst	172.20.120.25
Dst Interface	lan	Dst NAT IP	192.168.1.200
Dst NAT Port	554	Dst Port	554
Duration	5899	Level	notice
Log ID	13	Policy ID	5
Protocol	6	Received	1617
Received Packets	8	Sent	1819
Sent / Received	1.78 KB / 1.58 KB	Sent Packets	9
Sequence Number	25233	Service	RTSP
Source Country	Reserved	Src	172.20.120.21
Src Interface	wan1	Src Port	63004
Status	close	Sub Type	forward
Threat		Timestamp	September-05-13 10:28:03 AM
Tran Display	dnat	Virtual Domain	root

# Security Policies & Firewall Objects

Security policies and firewall objects are used to tell the FortiGate unit which traffic should be allowed and which should be blocked.

No traffic can pass through a FortiGate unit unless specifically allowed to by a security policy. With a security policy, you can control the addresses and services used by the traffic and apply various features, such as security profiles, authentication and VPNs.

Firewall objects are those elements within the security policy that further dictate how and when network traffic is routed and controlled. This includes addresses, services, and schedules.

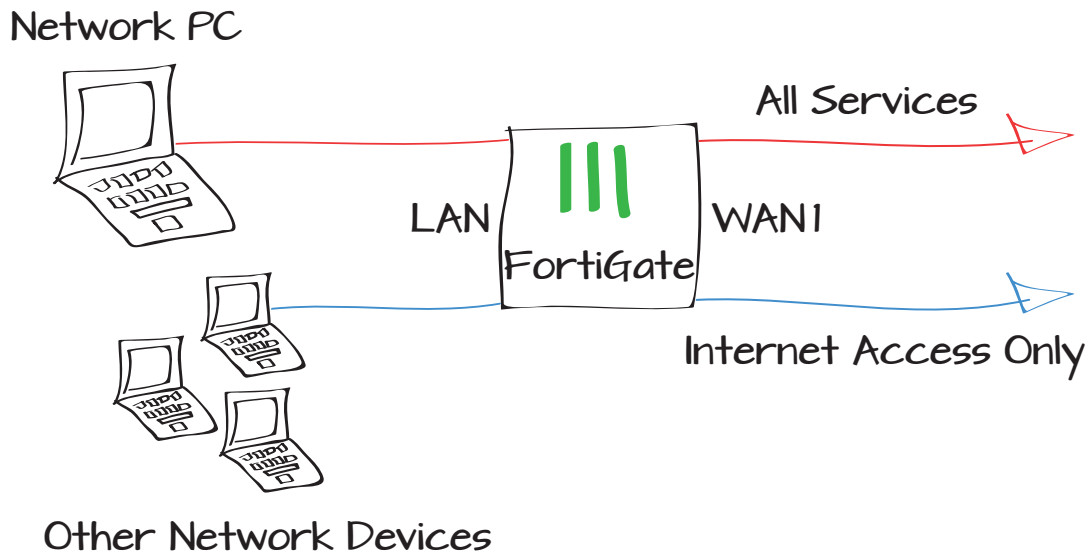
This section contains the following examples:

- Ordering security policies to allow different access levels
- Using port forwarding on a FortiGate unit
- Using AirPlay with iOS, AppleTV, FortiAP, and a FortiGate unit
- Using AirPrint with iOS and OS X and a FortiGate unit

# Ordering security policies to allow different access levels

This example illustrates how to order multiple security policies in the policy table, in order for the appropriate policy to be applied to different network traffic. In the example, three policies will be used: one that allows a specific PC access to all services, one that allows only Internet access to other network devices, and the default deny policy.

1. Configuring the Internet access only policy
2. Creating the policy for the PC
3. Ordering the policy table
4. Results



## Configuring the Internet access only policy

Go to **Policy > Policy > Policy**.

The screen that appears is the policy list. In the example, **Global View** has been selected, with the **Seq.#**, **From**, **To**, **Source**, **Destination**, **Action**, **Service**, and **Sessions** columns visible. To change the visible columns, right-click on the menu bar and select only the columns you wish to see.

Edit the first policy, which allows outgoing traffic. Set **Service** to **HTTP**, **HTTPS** and **DNS**. This policy now only allows Internet access.

Seq.#	From	To	Source	Destination	Action	Service	Sessions
1	lan	wan1	all	all	Accept	ALL	285
2	any	any	any	any	Deny	ALL	

Policy Type: ☒ Firewall ☐ VPN

Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface: lan

Source Address: all

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: HTTP, HTTPS, DNS

Action: ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

## Creating the policy for the PC

Go to **System > Network > Interfaces**.

Edit the LAN interface. Under **DHCP Server**, expand the **Advanced** options.

Create a new **MAC Address Access Control List**. Set **MAC** to the MAC address of the PC and **IP** to an available IP address.

This will automatically assign the specified

MAC	IP or Action
c4:2c:03:21:af:04	192.168.100.200
Unknown MAC Addresses	Assign IP

IP address to the PC when it connects to the FortiGate.

Go to **Firewall Objects > Address > Addresses**.

Create a new address. Set **Type** to **IP Subnet**, **Subnet/IP Range** to the IP address that will be assigned to the PC, and **Interface** to LAN.



Using /32 as the Netmask ensures that the firewall address applies only to the specified IP.

Go to **Policy > Policy > Policy**.

Create a new policy. Set **Incoming Interface** to LAN, **Source Address** to the PC address, and **Outgoing Interface** to WAN1.

## Ordering the policy table

Use the PC to browse to any Internet site, then go to **Policy > Policy > Policy**.

The policy with **Seq.#** 1 is the Internet access only policy, while 2 is the policy for the PC. The **Sessions** column shows that all sessions are currently using the Internet access policy. Policy 3 is the default deny policy.

To ensure that traffic from the PC matches

Category ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Type

Subnet / IP Range

Interface

Show in Address List ☒

Comments  0/255

Policy Type ☒ Firewall ☐ VPN

Policy Subtype ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface  +

Source Address  +

Outgoing Interface  +

Destination Address  +

Schedule

Service  +

Action

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

Seq.#	From	To	Source	Destination	Action	Service	Sessions
1	lan	wan1	all	all	Accept	HTTP HTTPS DNS	4
2	lan	wan1	Network_PC	all	Accept	ALL	0
3	any	any	any	any	Deny	ALL	

the PC policy, not the Internet access only policy, select the **Seq.#** column and drag the policy to the top of the list.

The device identity list will now appear at the top of the list. After the list is refreshed, this policy will be assigned **Seq.# 1**.

With this new order set, the FortiGate unit will attempt to apply the policy for the PC to all traffic from the LAN interface. If the traffic comes from a different source, the FortiGate will attempt to apply the Internet access only policy. If this attempt also fails, traffic will be blocked using the default deny policy.

When ordering multiple security policies, the most specific policies (in this case, the policy for the PC) must go to the top of the list, to ensure that the FortiGate unit checks them first when determining which policy to apply.

## Results

Browse the Internet using the PC and another network device, then refresh the policy list. You can now see **Sessions** occurring for both policies.

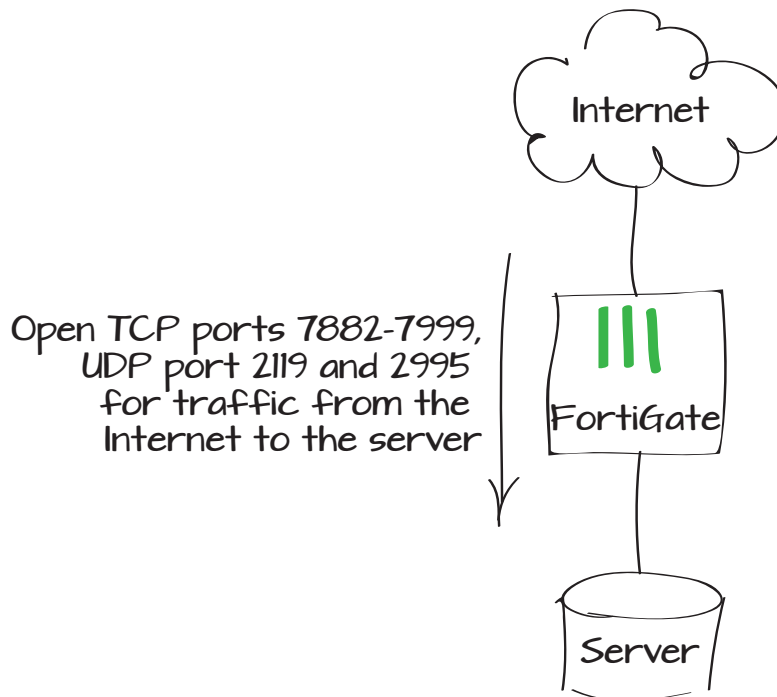
Seq.#	From	To	Source	Destination	Action	Service	Sessions
2	lan	wan1	Network_PC	all	Accept	ALL	0
1	lan	wan1	all	all	Accept	HTTP HTTPS DNS	4
3	any	any	any	any	Deny	ALL	

Seq.#	From	To	Source	Destination	Action	Service	Sessions
1	lan	wan1	Network_PC	all	Accept	ALL	38
2	lan	wan1	all	all	Accept	HTTP HTTPS DNS	44
3	any	any	any	any	Deny	ALL	

# Using port forwarding on a FortiGate unit

This example illustrates how to use virtual IPs to configure port forwarding on a FortiGate unit, which redirects traffic from one port to another. In this example, incoming connections from the Internet are allowed access to a server on the internal network by opening TCP ports in the range 7882 to 7999 and UDP ports 2119 and 2995.

1. Creating three virtual IPs
2. Adding the virtual IPs to a VIP group
3. Creating a security policy
4. Results





# Creating three virtual IPs

Go to **Firewall Objects > Virtual IPs > Virtual IPs.**

Enable **Port Forwarding** and add a virtual IP using TCP protocol with the range 7882-7999.

Create a second virtual IP for the UDP port 2119.

Create a third a virtual IP for the UDP port 2995.

Name	Port range VIP	
Comments	Write a comment... 0/255	
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.23	- 172.20.120.23
Mapped IP Address/Range	192.168.1.200	- 192.168.1.200
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	7882	- 7999
Map to Port	7882	- 7999

Name	First UDP Port VIP	
Comments	Write a comment... 0/255	
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.23	- 172.20.120.23
Mapped IP Address/Range	192.168.1.200	- 192.168.1.200
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	2119	- 2119
Map to Port	2119	- 2119

Name	Second UDP Port VIP	
Comments	Write a comment... 0/255	
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.23	- 172.20.120.23
Mapped IP Address/Range	192.168.1.200	- 192.168.1.200
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	2995	- 2995
Map to Port	2995	- 2995

## Adding virtual IPs to a VIP group

Go to **Firewall Objects > Virtual IPs > VIP Groups**.

Create a VIP group that includes all three virtual IPs.

Group Name:

Comments:  0/255

Color: [Change]

Interface:

Available VIPs:

Members:

First UDP Port VIP  
Port range VIP  
Second UDP Port VIP

## Creating a security policy

Go to **Policy > Policy > Policy**.

Create a security policy allowing inbound connections to the server from the Internet. Set the **Destination Address** as the new VIP group.

Policy Type: ☒ Firewall ☐ VPN

Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface:

Source Address:

Outgoing Interface:

Destination Address:

Schedule:

Service:

Action:

☐ Enable NAT

**Logging Options**

☐ No Log

☐ Log Security Events

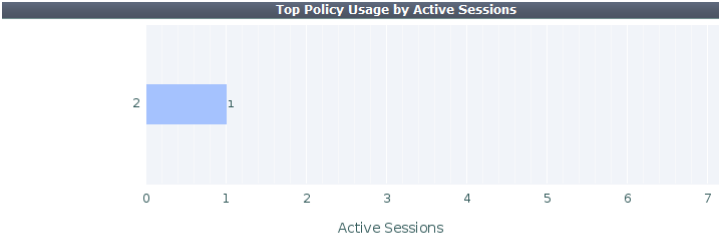
☒ Log all Sessions

# Results

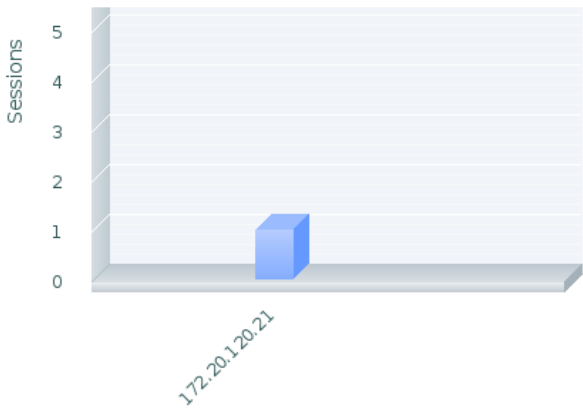
Go to **Policy > Monitor > Policy Monitor** to see the active sessions.

Select the blue bar for more information on a session.

Go to **Log & Report > Traffic Log > Forward Traffic** to see the logged activity.




Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
2	wan1	lan	✓	1	544 B	12



Src Interface	Dst Interface	Src	Dst	Policy ID	Serv
wan1	lan	172.20.120.21	172.20.120.23	2	7882/tc
wan1	lan	172.20.120.21	172.20.120.23	2	7882/tc
wan1	lan	172.20.120.21	172.20.120.23	2	7882/tc
wan1	lan	172.20.120.21	172.20.120.23	2	7882/tc
wan1	lan	172.20.120.21	172.20.120.23	2	7882/tc

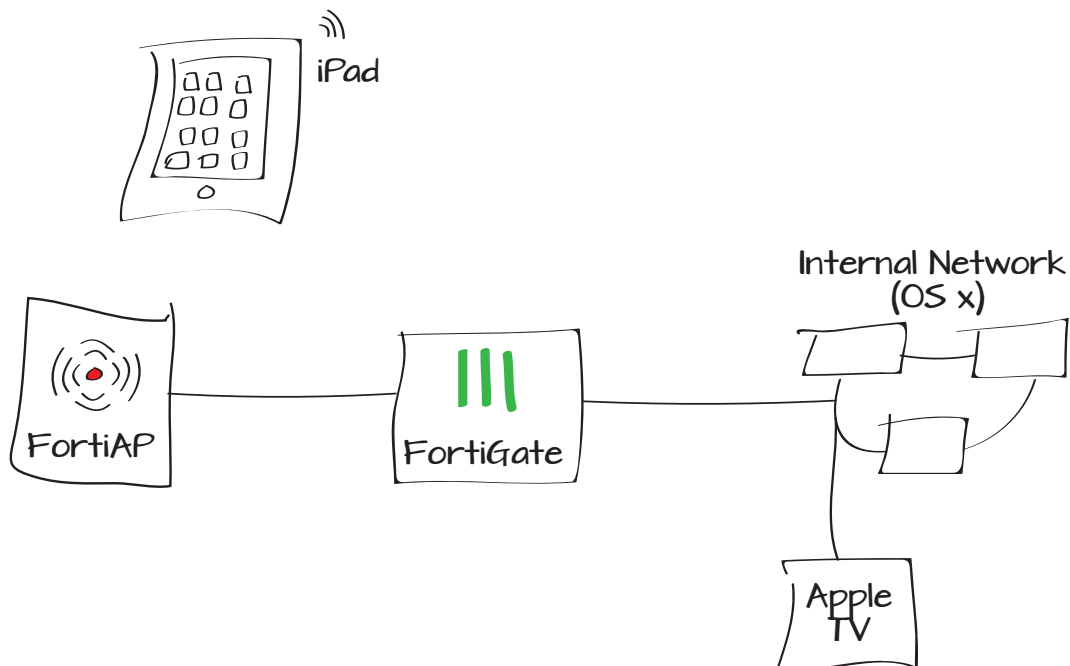
Select an entry for more information about the session.

Dst	172.20.120.23	Virtual Domain	root
Received	40	Source Country	Reserved
Sent / Received	48 B / 40 B	Dst NAT Port	7882
Duration	121	Sent	48
Application Detail:		Service	7882/tcp
Protocol	6	Destination Country	Reserved
Dst Port	7882	roll	65530
Status	timeout	Timestamp	Wed Mar 27 11:13:28 2013
Tran Display	dnat	Sequence Number	101294
Policy ID	2	Src Interface	wan1
Src	172.20.120.21	Dst NAT IP	192.168.1.200
Sent Packets	1	Level	notice 
Src Port	55045	Log ID	13
Sub Type	forward	Threat	
Received Packets	1	Date/Time	11:13:28 (Wed Mar 27 11:13:28 2013)
Dst Interface	lan		

# Using AirPlay with iOS, AppleTV, FortiAP, and a FortiGate unit

This example sets up AirPlay services for use with an iOS device using Bonjour and multicast security policies.

1. Configuring the FortiAP and SSIDs
2. Adding addresses for the wireless network
3. Adding service objects for multicasting
4. Adding multicast security policies
5. Adding inter-subnet security policies
6. Results



# Configuring the FortiAP and SSIDs

Go to **System > Network > Interfaces**.

Edit the internal interface to be used for the FortiAP and set **Addressing Mode** to **Dedicate to FortiAP**.

Connect the FortiAP unit to the FortiGate unit.

Go to **WiFi Controller > Managed Access Points > Managed FortiAP** and authorize the FortiAP.

Once authorized, it will appear in the authorized list.

Name

dmz (00:09:0F:99:39:6B)

Alias

Link Status

Up

Type

Physical Interface

Addressing mode

☐ Manual

☐ DHCP

☐ PPPoE

☒ Dedicate to FortiAP/F

IP/Network Mask

10.10.100.1/255.255.255.0

1 Connected FortiAPs/FortiSwitches

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☒ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

Device Management

Detect and Identify Devices

☐

Comments

Write a comment...

0/255

Administrative Status

☒ Up

☐ Down

Mesh	Access Point		State	Connected Via	SSID
	FAP22B3U11022065	<div><div>Edit</div><div>Delete</div><div>Authorize</div><div>Restart</div><div>Upgrade</div></div>		10.10.100.2	Radio 1: Radio 2:

Mesh	Access Point	State	Connected Via	SSIDs	Channel
	FAP22B3U11022065		10.10.100.2	Radio 1: All Radio 2: All	Radio 1: 1 Radio 2: 1

Go to **WiFi Controller > WiFi Network > SSID**.

Create a WiFi SSID for the network for wireless users and enable **DHCP Server**.

Adding addresses for the wireless network

Go to **Firewall Objects > Address > Addresses**.

Create an address for SSID 1.

Name

WLAN1

Type

WiFi SSID

Traffic Mode

Tunnel to Wireless Controller

IP/Network Mask

10.10.10.1/255.255.255.0

IPv6 Address

:::0

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
10.10.10.2	10.10.10.254

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Specify

Advanced...

WiFi Settings

SSID

SSID1

Security Mode

WPA/WPA2-Personal

Data Encryption

☒ AES ☐ TKIP ☐ TKIP-AES

Pre-shared Key

.....(8 - 63 characters)

Block Intra-SSID Traffic

☐

Maximum Clients

☐

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

SSID1\_Subnet

Color

[Change]

Type

Subnet

Subnet / IP Range

10.10.10.0/255.255.255.0

Interface

WLAN1 (SSID: SSID1)

Show in Address List

☒

Comments

Write a comment...

0/255

Create a second address for the internal network containing the OS X computers.

## Adding two service objects for AirPlay

Go to **Firewall Objects > Service > Services**.

Add service objects for each device connection.

Category

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Comments

Address

IPv6 Address

Multicast Address

Internal network

[Change]

IP Range

192.168.1.110-192.168.1.210

lan

☒

Wired and Wireless devices26/255

Name

Comments

Color

Show in Service List

Category

Protocol Type

IP/FQDN

AirPlay - Apple TV to iOS

Write a comment...0/255

[Change]

☒

Uncategorized

TCP/UDP/SCTP

	Destination Port		Source Port	
	Low	High	Low	High
TCP	7000	-		
UDP	1	- 65535		

Name

Comments

Color

Show in Service List

Category

Protocol Type

IP/FQDN

AirPlay - iOS to apple TV

Write a comment...0/255

[Change]

☒

Uncategorized

TCP/UDP/SCTP

	Destination Port		Source Port	
	Low	High	Low	High
TCP	7000	-		
TCP	7100	-		
TCP	49152	- 50000		
UDP	1	- 65535		



# Adding multicast security policies

Go to **Policy > Policy > Multicast Policy**.

Create a policy to allow multicast traffic from the LAN and WLAN1 for AppleTV to iOS devices. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to the SSID, and **Destination Address** to **Bonjour**.



The Bonjour address allows the devices to find each other when they connect through the FortiGate unit.

Go to **Policy > Policy > Multicast Policy**.

Create a policy to allow multicast traffic from the WLAN1 and LAN for iOS devices to AppleTV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, **Outgoing Interface** to LAN, and **Destination Address** to **Bonjour**.

Incoming Interface	lan
Source Address	Internal network
Outgoing Interface	WLAN1 (SSID: SSID1)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet
Outgoing Interface	lan
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

# Adding inter-subnet security policies

Go to **Policy > Policy > Policy**.

Create a policy allowing traffic from the Apple TV to the iOS device. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, and **Outgoing Interface** to the SSID.

Create a policy allowing traffic from the iOS device to the Apple TV. Set **Incoming Interface** to the SSID, **Source Address** to the SSID IP, and **Outgoing Interface** to the LAN.

## Results

Use Airplay from the iPad to stream video to the Apple TV.

Go to **Log & Report > Traffic Log > Multicast Traffic** to see the multicast traffic between the WLAN1 and LAN interfaces.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☐ Enable NAT

Firewall

VPN

Address

User Identity

Device Identity

lan

Internal network

WLAN1 (SSID: SSID1)

SSID1\_Subnet

always

AirPlay - Apple TV to iOS

ACCEPT

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☐ Enable NAT

Firewall

VPN

Address

User Identity

Device Identity

WLAN1 (SSID: SSID1)

SSID1\_Subnet

lan

Internal network


always


AirPlay - iOS to apple TV

ACCEPT

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Application Name	
4	09:49:41	WLAN1	lan	10.10.10.3	224.0.0.251	Unknown	3
5	09:47:28	lan	WLAN1	192.168.1.112	224.0.0.251	Unknown	2

Select an entry for more information.

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	300 B / 0 B	Duration	1237
Sent	300	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65498	Status	✓
Timestamp	Tue Apr 23 09:49:41 2013	Tran Display	noop
Sequence Number	0	Policy ID	5
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	3	Level	notice 
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	
Received Packets	0	Date/Time	09:49:41 (Tue Apr 23 09:49:41 2013)
Dst Interface	lan		

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	232 B / 0 B	Duration	1105
Sent	232	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65498	Status	✓
Timestamp	Tue Apr 23 09:47:28 2013	Tran Display	noop
Sequence Number	0	Policy ID	6
Src Interface	lan	Src	192.168.1.112
Sent Packets	1	Level	notice 
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	
Received Packets	0	Date/Time	09:47:28 (Tue Apr 23 09:47:28 2013)
Dst Interface	WLAN1		

Go to **Log & Report > Traffic Log > Log Forward** and filter policy IDs 6 and 7, which allow AirPlay traffic.

#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst	▼ Pol
▶ 1	10:30:09	lan	WLAN1	192.168.1.110	10.10.10.3	7
2	10:28:24	lan	WLAN1	192.168.1.110	10.10.10.3	7
3	10:27:14	WLAN1	lan	10.10.10.3	192.168.1.110	6
4	10:26:34	WLAN1	lan	10.10.10.3	192.168.1.110	6
5	10:25:55	WLAN1	lan	10.10.10.3	192.168.1.110	6
6	10:25:25	WLAN1	lan	10.10.10.3	192.168.1.110	6
7	10:25:13	WLAN1	lan	10.10.10.3	192.168.1.110	6
8	10:24:46	WLAN1	lan	10.10.10.3	192.168.1.110	6
9	10:24:01	WLAN1	lan	10.10.10.3	192.168.1.110	6
10	10:24:01	WLAN1	lan	10.10.10.3	192.168.1.110	6

Select an entry for more information.



Apple TV can also be connected to the Internet wirelessly. AirPlay will function from any iOS device connected to the same SSID as Apple TV. No configuration is required on the FortiGate unit.

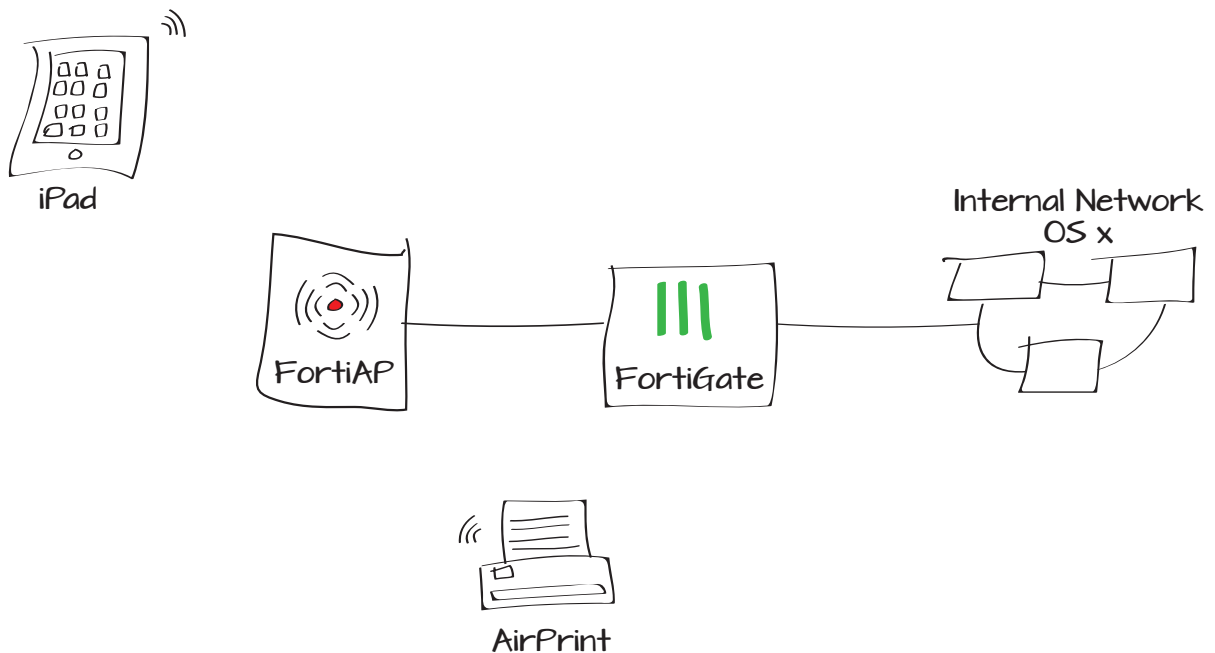
Dst	10.10.10.3	Virtual Domain	root
Received	2888	Source Country	Reserved
Sent / Received	2.82 KB / 2.82 KB	Duration	282
Sent	2888	Application Details	
Service	7010/udp	Protocol	17
Destination Country	Reserved	Dst Port	7010
roll	65498	Status	✓
Timestamp	Tue Apr 23 10:30:09 2013	Tran Display	noop
Sequence Number	10683	Policy ID	7
Src Interface	lan	Src	192.168.1.110
Sent Packets	38	Level	notice <span>     </span>
Src Port	7011	Log ID	13
Sub Type	forward	Threat	
Received Packets	38	Date/Time	10:30:09 (Tue Apr 23 10:30:09 2013)
Dst Interface	WLAN1		

Dst	192.168.1.110	Virtual Domain	root
Received	87986	Source Country	Reserved
Sent / Received	7.26 MB / 85.92 KB	Duration	28
Sent	7612538	Application Details	
Service	AirPlay	Protocol	6
Destination Country	Reserved	Dst Port	7100
roll	65498	Status	close
Timestamp	Tue Apr 23 10:27:14 2013	Tran Display	noop
Sequence Number	10994	Policy ID	6
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	5425	Level	notice <span>     </span>
Src Port	49625	Log ID	13
Sub Type	forward	Threat	
Received Packets	1667	Date/Time	10:27:14 (Tue Apr 23 10:27:14 2013)
Dst Interface	lan		

# Using AirPrint with iOS and OS X and a FortiGate unit

This example sets up AirPrint services for use with an iOS device and OS X computers using Bonjour and multicast security policies.

1. Configuring the FortiAP and SSIDs
2. Adding addresses for the wireless networks and printer
3. Adding service objects for printing
4. Adding multicast security policies
5. Adding inter-subnet security policies
6. Results



# Configuring the FortiAP and SSIDs

Go to **System > Network > Interfaces**.

Set an internal interface as dedicated to the FortiAP unit.

Connect the FortiAP unit to the FortiGate unit.

Go to **WiFi Controller > Managed Access Points > Managed FortiAP** and authorize the FortiAP.

Once authorized, it will appear in the authorized list.

Name

dmz (00:09:0F:99:39:6B)

Alias

Link Status

Up

Type

Physical Interface

Addressing mode

☐ Manual

☐ DHCP

☐ PPPoE

☒ Dedicate to FortiAP/FortiSwitch

IP/Network Mask

10.10.100.1/255.255.255.0

1 Connected FortiAPs/FortiSwitches

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☒ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

Device Management

☐ Detect and Identify Devices

Comments

Write a comment...

0/255

Administrative Status

☒ Up

☐ Down

Mesh	Access Point	State	Connected Via	SSIDs
-	FAP22B3U11022065		10.10.100.2	Radio 1: All Radio 2: All

- Edit
- Delete
- Authorize
- Restart
- Upgrade

Mesh	Access Point	State	Connected Via	SSIDs	Chann
■	FAP22B3U11022065		10.10.100.2	Radio 1: All Radio 2: All	Radio 1: 3 Radio 2: (

Go to **WiFi Controller > WiFi Network > SSID**.

Create a WiFi SSID for the network for wireless users and enable **DHCP Server**.

Name	WLAN1				
Type	WiFi SSID				
Traffic Mode	Tunnel to Wireless Controller				
IP/Network Mask	10.10.10.1/255.255.255.0				
IPv6 Address	::/0				
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access				
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET				
DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<div><div>Create New Edit Delete</div><table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.10.2</td><td>10.10.10.254</td></tr></tbody></table></div>	Starting IP	End IP	10.10.10.2	10.10.10.254
Starting IP	End IP				
10.10.10.2	10.10.10.254				
Netmask	255.255.255.0				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify				
<a href="#">Advanced...</a>					
WiFi Settings					
SSID	SSID1				
Security Mode	WPA/WPA2-Personal				
Data Encryption	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP-AES				
Pre-shared Key	..... (8 - 63 characters)				

Create an SSID for the network for the AirPrint printer and enable **DHCP Server**.

Adding addresses for the wireless networks and printer

Go to **Firewall Objects > Address > Addresses**.

Create addresses for the SSID1, SSID2, and AirPrint printer.

Name

WLAN2

Type

WiFi SSID

Traffic Mode

Tunnel to Wireless Controller

IP/Network Mask

20.20.20.1/255.255.255.0

IPv6 Address

::/0

Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
20.20.20.2	20.20.20.254

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP

☐ Specify

DNS Server

☒ Same as System DNS

☐ Specify

Advanced...

WiFi Settings

SSID

SSID2

Security Mode

WPA/WPA2-Personal

Data Encryption

☒ AES

☐ TKIP

☐ TKIP-AES

Pre-shared Key

•••••

(8 - 63 characters)

Category

☒ Address

☐ IPv6 Address

☐ Multicast Address

Name

SSID1\_Subnet

Color

[Change]

Type

Subnet

Subnet / IP Range

10.10.10.0/255.255.255.0

Interface

WLAN1 (SSID: SSID1)

Show in Address List

☒

Comments

Write a comment...

0/255

Category

☒ Address

☐ IPv6 Address

☐ Multicast Address

Name

SSID2\_Subnet

Color

[Change]

Type

Subnet

Subnet / IP Range

20.20.20.0/255.255.255.0

Interface

WLAN2 (SSID: SSID2)

Show in Address List

☒

Comments

Write a comment...

0/255



Create an address for the internal network containing the OS X computers.

# Adding service objects for printing

Go to **Firewall Objects > Service > Services**.

Create a new service for Internet Printing Protocol (IPP) for iOS devices.

Create a new service for PDL Data Stream for OS X computers.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

AirPrint Printer IP

Color

[Change]

Type

Subnet

Subnet / IP Range

20.20.20.2

Interface

WLAN2 (SSID: SSID2)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal network

Color

[Change]

Type

IP Range

Subnet / IP Range

192.168.1.110-192.168.1.210

Interface

lan

Show in Address List

☒

Comments

Wired and Wireless devices 26/255

Name

IPP

Comments

Internet Printing Protocol 26/255

Color

[Change]

Show in Service List

☒

Category

Uncategorized

Protocol Type

TCP/UDP/SCTP

IP/FQDN

Protocol

TCP

Destination Port

Low 631 High -

Source Port

Low High -

Name

PDL

Comments

PDL Data Stream 15/255

Color

[Change]

Show in Service List

☒

Category

General

Protocol Type

TCP/UDP/SCTP

IP/FQDN

Protocol

TCP

Destination Port

Low 9100 High -

Source Port

Low High -

## Adding multicast security policies

Go to **Policy > Policy > Multicast Policy**.

Create two policies to allow multicast traffic from WLAN1 and WLAN2 for iOS devices.

For the first policy, set **Incoming Interface** to WLAN1, **Source Address** to the SSID1 IP, **Outgoing Interface** to WLAN2, and **Destination Address** to **Bonjour**.

For the second policy, set **Incoming Interface** to WLAN2, **Source Address** to the SSID2 IP, **Outgoing Interface** to WLAN1, and **Destination Address** to **Bonjour**.



The Bonjour address allows the devices to find each other when they connect through the FortiGate unit.

Create two policies to allow multicast traffic from the LAN and WLAN2 for OS X computers.

For the first policy, set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to WLAN2, and **Destination Address** to **Bonjour**.

Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	WLAN2 (SSID: SSID2)
Source Address	SSID2_Subnet
Outgoing Interface	WLAN1 (SSID: SSID1)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Incoming Interface	lan
Source Address	Internal network
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

For the second policy, set **Incoming Interface** to WLAN2, **Source Address** to the AirPrint, **Outgoing Interface** to LAN, and **Destination Address** to Bonjour.

## Adding inter-subnet security policies

Go to **Policy > Policy > Policy**.

Create a policy allowing printing from wireless devices. Set **Incoming Interface** to WLAN1, **Source Address** to the SSID1 IP, **Outgoing Interface** to WLAN2, **Destination Address** to the AirPrint, and **Service** to IPP.

Create a policy allowing printing from an OS X computer to the AirPrint printer. Set **Incoming Interface** to LAN, **Source Address** to the Internal network, **Outgoing Interface** to WLAN2, **Destination Address** to the AirPrint, and **Service** to IPP.

Incoming Interface	WLAN2 (SSID: SSID2)
Source Address	AirPrint Printer IP
Outgoing Interface	lan
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	

Policy Type	Firewall VPN
Policy Subtype	Address User Identity Device Identity
Incoming Interface	WLAN1 (SSID: SSID1)
Source Address	SSID1_Subnet
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	AirPrint Printer IP
Schedule	always
Service	IPP
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	Firewall VPN
Policy Subtype	Address User Identity Device Identity
Incoming Interface	lan
Source Address	Internal network
Outgoing Interface	WLAN2 (SSID: SSID2)
Destination Address	AirPrint Printer IP
Schedule	always
Service	PDL
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

# Results

Print a document from an iOS device.


Go to **Log & Report > Traffic Log > Multicast Traffic** to see the printing traffic passing through the FortiGate unit.

Select an entry to see more information.

Go to **Log & Report > Traffic Log > Forward Traffic** and verify the entry with the IPP service.

#	▾ Date/Time	▾ Src Interface	▾ Dst Interface	▾ Src	▾ Dst	▾ Policy ID	▾ Service
14	03-27 20:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
15	03-27 19:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
16	03-27 18:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
17	03-27 17:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
18	03-27 16:44	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
19	03-27 16:07	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
20	03-27 15:57	WLAN2	WLAN1	20.20.20.2	224.0.0.251	2	5353/udp
21	03-27 15:55	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
22	03-27 15:54	WLAN1	WLAN2	10.10.10.3	224.0.0.251	1	5353/udp
23	03-27 15:54	WLAN2	WLAN1	20.20.20.2	224.0.0.251	2	5353/udp

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	77 B / 0 B	Duration	17765
Sent	77	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65530	Status	✓
Timestamp	Wed Mar 27 20:44:11 2013	Tran Display	noop
Sequence Number	0	Policy ID	1
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	1	Level	notice <span>     </span>
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	
Received Packets	0	Date/Time	03-27 20:44 (Wed Mar 27 20:44:11 2013)
Dst Interface	WLAN2		

Dst	 20.20.20.2	Virtual Domain	root
Received	42012	Source Country	Reserved
Sent / Received	2.18 KB / 41.03 KB	Duration	2
Sent	2229	Application Details	
Service	631/tcp	Protocol	6
Destination Country	United States	Dst Port	631
roll	65530	Status	close
Timestamp	Wed Mar 27 15:35:41 2013	Tran Display	noop
Sequence Number	40762	Policy ID	3
Src Interface	WLAN1	Src	10.10.10.3
Sent Packets	27	Level	notice <span>     </span>
Src Port	52549	Log ID	13
Sub Type	forward	Threat	
Received Packets	34	Date/Time	03-27 15:35 (Wed Mar 27 15:35:41 2013)
Dst Interface	WLAN2		

Print a document from an OS X computer.

Go to **Log & Report > Traffic Log > Multicast Traffic** to see the printing traffic passing through the FortiGate unit.

Select an entry to see more information.

Go to **Log & Report > Traffic Log > Forward Traffic** and filter the destination interface for WLAN2 traffic.

Select an entry to see more information.

#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst	▼ Policy ID	▼ Service
1	13:09:28	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
2	12:09:28	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
3	11:09:29	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
4	10:32:57	lan	WLAN2	192.168.1.112	224.0.0.251	4	5353/udp
5	10:23:44	WLAN2	WLAN1	20.20.20.2	224.0.0.251	2	5353/udp
6	10:23:44	WLAN2	lan	20.20.20.2	224.0.0.251	3	5353/udp

Dst	224.0.0.251	Virtual Domain	root
Received	0	Source Country	Reserved
Sent / Received	120 B / 0 B	Duration	417
Sent	120	Application Details	
Service	5353/udp	Protocol	17
Destination Country	Reserved	Dst Port	5353
roll	65526	Status	✓
Timestamp	Mon Apr 1 10:21:23 2013	Tran Display	noop
Sequence Number	0	Policy ID	4
Src Interface	lan	Src	192.168.1.112
Sent Packets	2	Level	notice
Src Port	5353	Log ID	12
Sub Type	multicast	Threat	

Refresh Download Raw Log

#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst	▼ Policy ID	▼ Service
▶ 1	10:22:15	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
2	10:21:21	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
3	10:21:19	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100
4	10:21:08	lan	WLAN2	192.168.1.112	20.20.20.2	5	9100

Dst	20.20.20.2	Virtual Domain	root
Received	532	Source Country	Reserved
Sent / Received	40.45 KB / 532 B	Duration	55
Sent	41416	Application Details	
Service	9100/tcp	Protocol	6
Destination Country	United States	Dst Port	9100
roll	65526	Status	close
Timestamp	Mon Apr 1 10:22:15 2013	Tran Display	noop
Sequence Number	3444	Policy ID	5
Src Interface	lan	Src	192.168.1.112
Sent Packets	33	Level	notice
Src Port	57631	Log ID	13
Sub Type	forward	Threat	
Received Packets	10	Date/Time	10:22:15 (Mon Apr 1 10:22:15 2013)
Dst Interface	WLAN2		

# Security Features

Security features, including antivirus, web filtering, application control, intrusion protection (IPS), email filtering, and data leak prevention (DLP), apply core security functions to the traffic accepted by your FortiGate unit.

Each security feature has a default profile. You can also create custom profiles to meet the needs of your network. These profiles are then applied to your security policies and used to monitor and, if necessary, block external and internal traffic that is considered risky or dangerous.

This section contains the following examples:

- [Monitoring your network using client reputation](#)
- [Controlling network access using application control](#)
- [Using a custom signature to block web traffic from Windows XP](#)
- [Protecting a web server from external attacks](#)
- [Blocking outgoing traffic containing sensitive data](#)
- [Preventing credit card numbers from escaping your network](#)
- [Blocking access to specific websites](#)
- [Extra help: Web filtering](#)
- [Blocking HTTP and HTTPS traffic with web filtering](#)
- [Using web filter overrides to control website access](#)
- [Limiting access to personal interest websites using quotas](#)
- [Setting up YouTube for Education](#)
- [Inspecting traffic content using flow-based inspection](#)
- [Analyzing your network traffic using a one-armed sniffer](#)
- [Excluding specific users from security scanning](#)

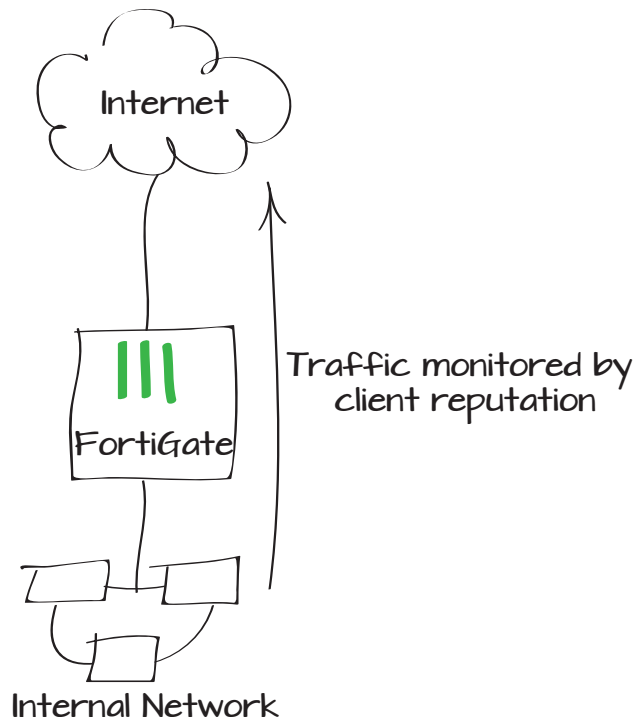
# Monitoring your network using client reputation

Client reputation allows you to monitor traffic as it flows through your FortiGate unit to identify users who may be engaging in risky or dangerous behavior. A variety of different areas can be monitored, depending on what concerns you have about activity on your network. In this example, particular attention will be given to any traffic containing peer-to-peer (P2P) downloading.



Client reputation only monitors risky activity, it does not block it. If you discover activity that you are concerned about, additional action must be taken to stop it, such as applying a more restrictive security policy to the traffic.

1. Enabling logging to disk
2. Enabling client reputation
3. Results



# Enabling logging to disk

In order to see your Client Reputation Tracking results, logging to disk must be enabled.

Go to **Log & Report > Log Config > Log Settings**. Under **Logging and Archiving**, enable **Disk**.

Logging and Archiving

☒ Disk

☐ Enable Local Reports

☐ Send Logs to FortiAnalyzer/FortiManager

IP Address:  Test Connectivity

☐ Send Logs to FortiCloud

Account:  Test Connectivity

☐ Event Logging

# Enabling client reputation

Go to **Security Profiles > Client Reputation > Threat Level Definition**.

Enable **Client Reputation Tracking**. Assign a **Risk Level Value** for each category, based on your traffic concerns and needs. In the example, the value for **P2P Applications** has been raised to **Critical**. All other categories have been left at their default level.

ON Client Reputation Tracking

Application Protection

☐

 Botnet Applications

☐

 P2P Applications

☐

 Proxy Applications

☐

 Games Applications

Intrusion Protection

☐

 Critical Severity Attack Detected

☐

 High Severity Attack Detected

☐

 Medium Severity Attack Detected

☐

 Low Severity Attack Detected

☐

 Informational Severity Attack Detected

Risk Level Values

LOW

5

MED

10

HIGH

30

CRIT

50

Malware Protection

☐

 Malware Detected

☐

 Botnet Connection Detected

Packet Based Inspection

☐

 Blocked by Firewall Policy

☐

 Failed Connection Attempts

Web Activity

☐

 All Blocked URLs

☐

 Visit to Security Risk Sites

☐

 Visit to Potentially Liable Sites

☐

 Visit to Adult/Mature Content Sites

☐

 Visit to Bandwidth Consuming Sites



Enabling client reputation also enables the **Log Allowed Traffic** setting for all security policies. For more information, see “[Logging network traffic to gather information](#)” on page 39.



# Results

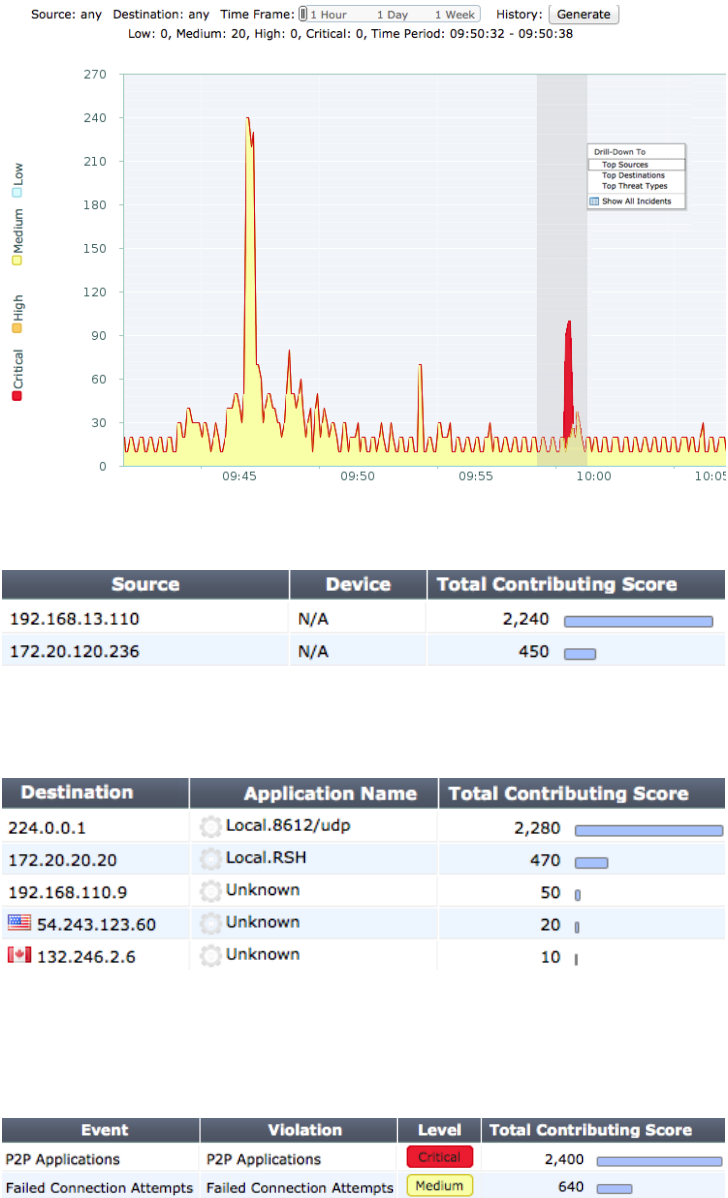
After traffic has been monitored for a day, go to **System > Dashboard > Threat History** to view the **Threat History** widget, which shows a graph of monitored threats.

Any sections in red should be examined, as they contain threats that are considered **Critical**. To select this section, click on its left side and then click on the right side. Select a **Drill-Down** option to view more information about the traffic and the client reputation scores (the higher the score, the riskier the behaviour).

**Top Sources** shows the sources of the risky behaviour on your network.

**Top Destinations** shows the destinations which have caused the risks.

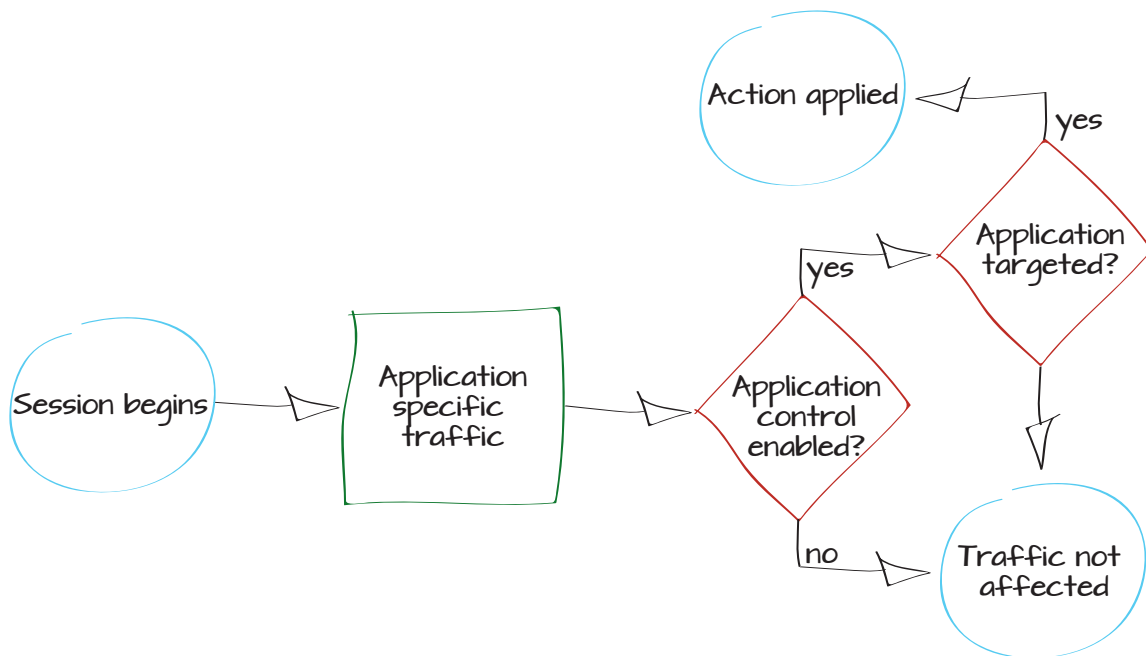
**Top Threat Types** shows the threat category and the risk level of the behaviour.



# Controlling network access using application control

This example uses application control to monitor traffic and determine what applications are contributing to high bandwidth usage or distracting employees. After this is determined, a different application sensor is used to block those applications from having network access.

1. Creating an application sensor to monitor network traffic
2. Adding the monitoring sensor to a security policy
3. Reviewing the application control monitor
4. Creating an application sensor to block applications
5. Adding the blocking sensor to a security policy
6. Results



# Creating an application control sensor to monitor traffic

Go to **Security Profiles > Application Control > Application Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor list for monitoring application traffic.

Select **Create New** to add a new application filter. Leave all **Filter Options** selected.

Ensure that you set the **Action** to **Monitor**. At this stage in the process, you are monitoring the traffic to locate any problems that may be occurring, rather than blocking applications.

Name

monitor\_application\_traffic

Comments

Comments

0/255

Sensor Type

Filter Based

Specify Applications

Filter Options

Category

☒ Botnet

☒ Game

☒ Media

☒ Proxy

☒ Storage.Backup

☒ eMail

☒ General.Interest

☒ Network.Service

☒ Remote.Access

☒ Update

☒ File.Sharing

☒ IM

☒ P2P

☒ Social.Networking

☒ VoIP

Popularity

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

Technology

☒ Browser-Based

☒ Client-Server

☒ Network-Protocol

☒ Peer-to-Peer

Risk

☒ Botnet

☒ Excessive-Bandwidth

☒ None

Application Name	Category	Technology	Popularity	Risk
012mail	eMail	Browser-Based	☆☆☆☆☆	
0zz0	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
1und1.Mail	eMail	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Browse.Upload.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Search.Download.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2ch	Social.Networking	Browser-Based	☆☆☆☆☆	
2ch_Post	Social.Networking	Browser-Based	☆☆☆☆☆	
3PC	Network.Service	Network-Protocol	☆☆☆☆☆	
4shared	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
6cn	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
9PFS	Network.Service	Network-Protocol	☆☆☆☆☆	
9PTV	P2P	Peer-to-Peer	☆☆☆☆☆	Excessive-Bandwidth
24lin	IM	Client-Server	☆☆☆☆☆	Excessive-Bandwidth
51.Com	Social.Networking	Browser-Based	☆☆☆☆☆	

1

/ 164

Total: 226

Action

Monitor

Block

Reset

Traffic Shaping

Controlling network access using application control

131

# Adding the monitoring sensor to a security policy

Go to **Policy > Policy > Policy**.

Edit the security policy that allows internal users to access the Internet. Under **Security Profiles**, enable **Application Control** and set it to use the new filter.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

☐ Fixed Port

Click to add...

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

ON

Application Control

monitor\_application\_traffic

# Reviewing the application control monitor

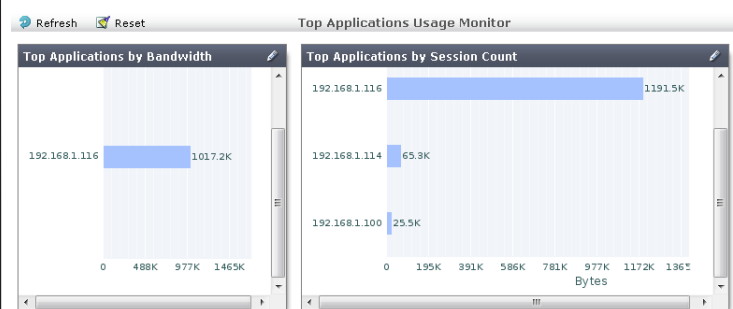
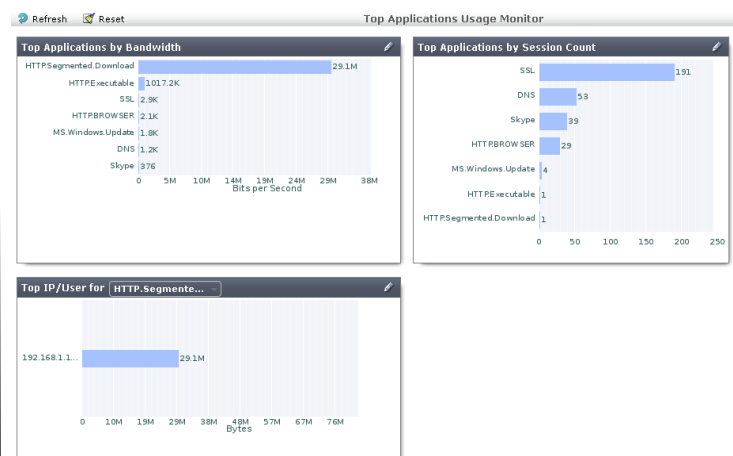
Go to **Security Profiles > Monitor > Application Monitor** to see the results found by the application sensor.

Select a bar to see further details on the usage statistics.

In the example, you can see an occurrence of an HTTP segmented download, which typically occurs during Peer-to-Peer (P2P) downloads. To avoid this from occurring in the future, P2P applications must be blocked.

# Creating an application sensor to block applications

Go to **Security Profiles > Application Control > Application Sensors** and create a new sensor list for blocking application traffic.



Name:

Comments:  0/255

Select **Create New** to add a new application filter.

In the **Category** list, select the application categories you wish to block. As well as blocking P2P, other types of applications can be selected that are known to distract employees.

Ensure that you set the **Action** to **Block**.

Sensor Type

☒ Filter Based

☐ Specify Applications

Filter Options

Category

☐ Botnet

☐ Game

☒ Media

☐ Proxy

☐ Storage.Backup

☐ eMail

☒ General.Interest

☐ Network.Service

☐ Remote.Access

☐ Update

☒ File.Sharing

☒ IM

☒ P2P

☒ Social.Networking

☐ VoIP

Popularity

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

☒ ☆☆☆☆☆

Technology

☒ Browser-Based

☒ Client-Server

☒ Network-Protocol

☒ Peer-to-Peer

Risk

☒ Botnet

☒ Excessive-Bandwidth

☒ None

Application Name	Category	Technology	Popularity	Risk
0zz0	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Browse.Upload.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2Shared.Search.Download.File	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
2ch	Social.Networking	Browser-Based	☆☆☆☆☆	
2ch_Post	Social.Networking	Browser-Based	☆☆☆☆☆	
4shared	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
6cn	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
9PTV	P2P	Peer-to-Peer	☆☆☆☆☆	Excessive-Bandwidth
24im	IM	Client-Server	☆☆☆☆☆	Excessive-Bandwidth
S1.Com	Social.Networking	Browser-Based	☆☆☆☆☆	
S1.Com_BBS	Social.Networking	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
S1.Com_Music	Media	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
S1.Com_Posting	Social.Networking	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth
S1.Com_Webdisk	File.Sharing	Browser-Based	☆☆☆☆☆	Excessive-Bandwidth

1 / 965

Action

☒ Monitor

☐ Block

☐ Reset

☐ Traffic Shaping

# Adding the blocking sensor to a security policy

Go to **Policy > Policy > Policy**.

Edit the firewall policy allowing internal users to access the Internet. Under **Security Profiles**, enable **Application Control** and set it to use the new filter.

Policy Type

☒ Firewall

☐ VPN

Policy Subtype

☒ Address

☐ User Identity

☐ Device Identity

Incoming Interface

internal

Source Address

all

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

☐ Fixed Port

Click to add...

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

ON

Application Control

Block\_app-sensor

# Results

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see the sensor is working and blocking the traffic from the selected application types, including the P2P application Skype.

Select an entry to view more information, including the application name and the device the traffic originated on.

	Application Name	Application Control List	Application Category	Application Control Acti
	Skype	Block_app-sensor	P2P	drop-session
2	Skype	Block_app-sensor	P2P	drop-session
	Skype	Block_app-sensor	P2P	drop-session
	Skype	Block_app-sensor	P2P	drop-session
		Block_app-sensor		

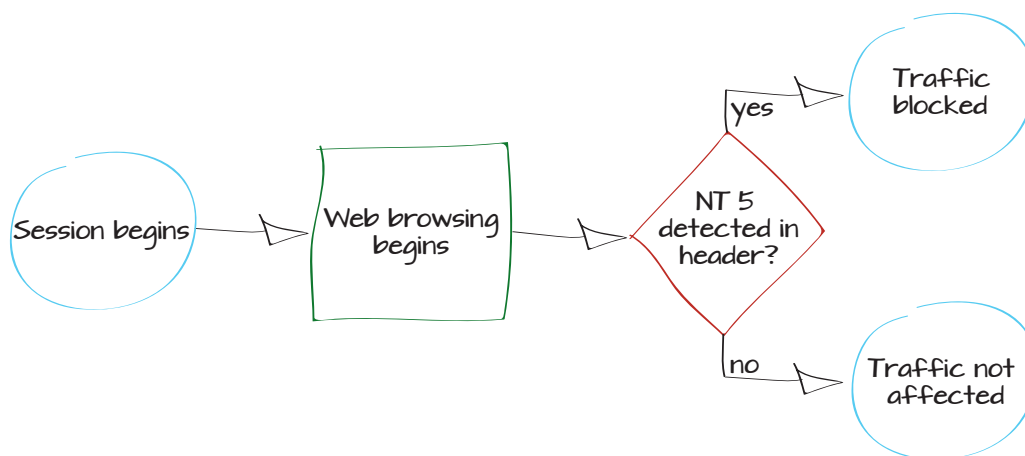
Dst	 157.55.56.147	Virtual Domain	root
Received	252	Source Country	Reserved
Application Name	 Skype	Src NAT IP	172.20.120.124
Sent / Received	248 B / 252 B	Device Type	Windows PC
Duration	88	Sent	248
Src NAT Port	5878	Application Details	
Device	 00:0c:29:4b:d7:cc	Service	40041/tcp
Protocol	6	byod_name	
Destination Country	United States	Application Control List	Block_app-sensor
Dst Port	40041	roll	65499
Status	deny	Timestamp	Wed Dec 5 22:36:10 2012
Application ID	10	OS Name	Windows
Sequence Number	13720	Policy ID	8
Src Interface	internal	Src	192.168.1.114
Level	notice 	Application Category	P2P
Src Port	5878	Application Control Action	drop-session
logid	13	Sub Type	forward
Threat		Tran Display	snat
Date/Time	1 minute ago (Wed Dec 5 22:36:10 2012)	Dst Interface	wan1

# Using a custom signature to block web traffic from Windows XP

When a computer's operating system lacks vendor support, it becomes a threat to the network because newly discovered exploits will not be patched. Using the FortiGate application control feature, you can choose to restrict these computers from accessing external resources.

This recipe shows how to use application control to block web traffic from PCs running on Windows operating systems using NT 5, including Windows XP and Windows Server 2003.

1. Creating a custom application control signature
2. Creating an application control sensor
3. Adding the sensor to the outbound traffic security policy
4. Results





## Creating a custom application control signature

Go to **Security Profiles > Application Control > Application List** and select **Create New**.

Use the following text to create the signature:



Make sure to remove all hard line breaks from the signature. To ensure all breaks have been removed, click and drag the bottom right corner of the signature box until the text appears in a single line.

```
F-SBID( --attack_id 8151;
--vuln_id 8151; --name "Windows.
NT.5.Web.Surfing"; --default
action drop_session; --service
HTTP; --protocol tcp; --app_
cat 25; --flow from client;
--pattern "Windows NT 5."; --no_
case; --context header; )
```

The signature will appear at the top of the application list and be listed in the **Web.Others** category.

## Creating an application sensor

Go to **Security Profiles > Application Control > Application Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.

Name	Windows.NT.5.Web.Su
Comments	<input type="text" value="Write a comment..."/> 0/255
Signature	<div>F-SBID( --attack_id 8151; --vuln_id 8151; --name "Windows.NT.5.Web.Surfing"; --default_action drop_session; --service HTTP; --protocol tcp; --app_cat 25; --flow from_client; --pattern "Windows NT 5."; --no_case; --context header; )</div> <div> Submit Signature</div>

Application Name	Category
APP Windows.NT.5.Web.Surfing	Web.Others

Name	Block Windows NT 5
Comments	<input type="text" value="Comments"/> 0/255
<input checked="" type="checkbox"/> Allow and Log DNS Traffic	

After selecting **OK**, select **Create New** to add the new signature.

In order to locate the correct signature, select **Show more...** under **Category**, then select only **Web.Others**.

Set **Sensor Type** to **Specify Applications**. The new signature will appear at the top of the list. Select the signature, then set **Action** to **Block**.

The signature will now appear as part of the sensor.

Sensor Type

☐ Filter Based

☒ Specify Applications

Filter Options

☒ Basic

☐ Advanced

Type to search applications

Application Name	Category
Windows.NT.5.Web.Surfing	Web.Others
1and1	Web.Others
5GBfree	Web.Others
A2hosting	Web.Others
AOL	Web.Others
AT&T.Synaptic	Web.Others
AffinityLive	Web.Others
AffinityLive_New.Project	Web.Others
Amazon.AWS_EC2	Web.Others
Android	Web.Others
Answerbase	Web.Others
Answerbase_Answer.Question	Web.Others
Answerbase_Ask.Question	Web.Others
Aplus	Web.Others

Action

Monitor

Block

Reset

Traffic Shaping

Name

Block Windows NT 5

Comments

Comments

0/255

☒ Allow and Log DNS Traffic

Create New

Edit

Delete

Insert

Category	Action	Application
Web.Others	Block	Windows.NT.5.Web.Surfing
	Monitor	All Other Known Applications
	Monitor	All Other Unknown Applications

## Adding the sensor to the outbound traffic security policy

Go to **Policy > Policy > Policy** and edit the policy controlling your outbound traffic.

Under **Security Policies**, enable **Application Control** and set it to use the new sensor. In order to also block HTTPS traffic, enable **SSL/SSH Inspection** and set it to use the **default** sensor.



Enabling SSL/SSH Inspection will cause web browsers to experience a certificate error. To avoid this, see [“Preventing security certificate warnings when using SSL inspection”](#) on page 290.

## Results

When a PC running one of the affected operating systems attempts to connect to the Internet using a browser, the connection will fail. This includes Windows virtual machines.

PCs running on other operating systems, including later versions of Windows, will not be affected.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	lan +
Source Address	all +
Outgoing Interface	wan1 +
Destination Address	all +
Schedule	always -
Service	ALL +
Action	ACCEPT -
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input checked="" type="radio"/> Log Security Events	
<input type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="checkbox"/> AntiVirus	default
<input type="checkbox"/> Web Filter	default
<input checked="" type="checkbox"/> Application Control	Block Windows NT 5 X
<input type="checkbox"/> IPS	default
<input type="checkbox"/> Email Filter	default
<input type="checkbox"/> DLP Sensor	default
<input checked="" type="checkbox"/> SSL/SSH Inspection	default X

Go to **Log & Report > Traffic Log > Forward Traffic** to see logs of the blocked traffic.

In the example, the blocked computer (IP address 192.168.100.112) was running Windows XP.



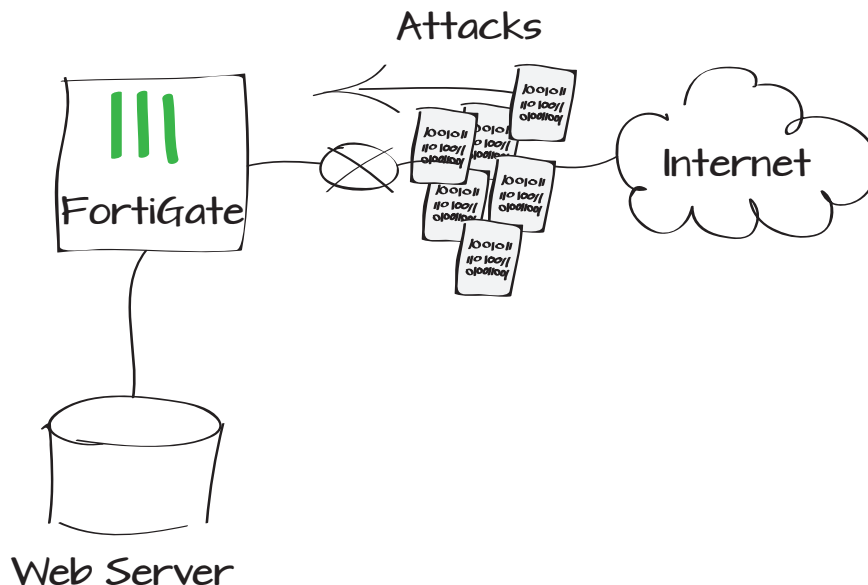
This recipe will only block web traffic from computers running the affected operating systems. If you wish to block these computers from being on the network entirely, further action will be necessary. However, the logs generated by this recipe can be used to identify the computers you wish to block.

#	Policy ID	Date/Time	Source	Destination	Security Event	Security Action
1	1	10:32:25	192.168.100.112	184.150.152.177 (img.youtube.com)	app-ctrl	✗
2	1	10:30:27	192.168.100.111	108.160.165.12 (www.dropbox.com)	app-ctrl	✗
3	1	08:43:27	192.168.100.112	173.194.64.100 (s.yimg.com)	app-ctrl	✗
4	1	10:17:33	192.168.100.112	213.180.204.25 (mail.yandex.com)	app-ctrl	✗
5	1	08:59:14	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	✗
6	1	08:58:36	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	✗
7	1	08:58:16	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	✗
8	1	08:57:00	192.168.100.112	87.250.250.25 (mail.yandex.com)	app-ctrl	✗
9	1	08:54:03	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	✗
10	1	08:53:09	192.168.100.112	31.13.69.128 (www.facebook.com)	app-ctrl	✗
11	1	08:52:42	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	✗
12	1	08:52:28	192.168.100.112	208.91.113.66 (support.fortinet.com)	app-ctrl	✗
13	1	08:50:00	192.168.100.112	173.194.64.100 (s.yimg.com)	app-ctrl	✗
14	1	08:50:00	192.168.100.112	173.194.64.100 (s.yimg.com)	app-ctrl	✗
15	1	08:48:35	192.168.100.112	23.41.245.231 (ocsp.entrust.net)	app-ctrl	✗
16	1	08:44:42	192.168.100.112	173.194.64.100 (s.yimg.com)	app-ctrl	✗
17	1	08:43:27	192.168.100.112	173.194.64.100 (s.yimg.com)	app-ctrl	✗

# Protecting a web server from external attacks

This example uses the FortiOS intrusion protection system (IPS) to protect a web server by configuring an IPS sensor to protect against common attacks and adding it to the policy which allows external traffic to access the server. A denial of service (DoS) security policy is also added to further protect the server against that specific type of attack.

1. Configuring an IPS sensor to protect against common attacks
2. Adding the IPS sensor to a security policy
3. Adding a DoS security policy
4. Results



# Configuring an IPS sensor to protect against common attacks

Go to **Security Profiles > Intrusion Protection > IPS Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.

Create a new IPS filter. Set the **Target** to **server** and set the **Action** to **Block All**.

Edit IPS SensorProtect\_my\_web\_Server

NameProtect\_my\_web\_server

CommentsWrite a comment...0/255

Create NewEditDeleteInsertMove ToView Rules

IDSeverityTargetOSActionPacket LoggingMatched Signatures

Apply

Sensor TypeFilter BasedSpecify Signatures

Filter Options

Severity

☒ critical  
☒ high  
☒ medium  
☒ low  
☒ info

Target

☐ client  
☒ server

OS

☒ BSD  
☒ Linux  
☒ MacOS  
☒ Other  
☒ Solaris  
☒ Windows

Name	Severity	Target	OS
2Wire.Wireless.Router.XSRF.Password.Reset	medium	server, client	Windows
3Com.3CDaemon.FTP.Server.Buffer.Overflow	high	server	Windows
3Com.Intelligent.Management.Center.Directory.Traversal	medium	server	Windows
3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Windows
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	Windows
4D.WebStar.FTP.Command.Buffer.Overflow	high	server	Windows
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	medium	server	Windows
7T.IGSS.ODBC.Server.Memory.Corruption	medium	server	Windows
7T.Interactive.Graphical.SCADA.File.Operations.Buffer.Overflow	high	server	Windows
7Technologies.IGSS.SCADA.System.Directory.Traversal	medium	server	Windows
427BB.Cookie.Based.Authentication.Bypass	medium	server	All
427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	All
1024CMS.Standard.PHP.File.Inclusion	high	server	Windows
ABB.Multiple.Products.RobNetScanHost.exe.Stack.Buffer.Overflow	critical	server	Windows

1 / 206 [ Total: 2877 ]

ActionSignature DefaultsMonitor AllBlock AllResetQuarantine

☒ Packet Logging

## Adding the IPS sensor to a security policy

Go to **Policy > Policy > Policy**. Edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** and set it to use the new sensor.

## Adding a DoS security policy

Go to **Policy > Policy > DoS Policy**.

Create a new policy. The **Incoming Interface** is your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☐ Enable NAT

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

wan1

all

lan

Web\_server

always

ALL

ACCEPT

Logging Options

☐ No Log

Incoming Interface

Source Address

Destination Address

Service

wan1

all

all

ALL

Anomalies				
Name	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	20
tcp_port_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
tcp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
tcp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
icmp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	250
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	100
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	300
icmp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000

# Results



**WARNING:** Causing a DoS attack is illegal, unless you own the server under attack. Before performing an attack, make sure you have the correct server IP.

Perform an DoS tcp\_sync\_flood attack to the web server IP address. IPS blocks the TCP sync session when it reaches the **tcp\_syn\_flood** threshold, in this case 20.

Go to **Log & Report > Security Log > Intrusion Protection** to view the results of the DoS policy.

Select an entry to view more information, including the severity of the attack and the attack name.

Intrusion Raw Log							
Severity	Src	Protocol	Count	Attack Name	Attack ID	Level	
critical	172.20.120.123	tcp	4	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	3	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	2	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	1	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	5	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	9	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	2	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	7	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	3	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	4	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	2	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	
critical	172.20.120.123	tcp	11	tcp_syn_flood	100663396	anomaly: tcp_syn_flood, 21	

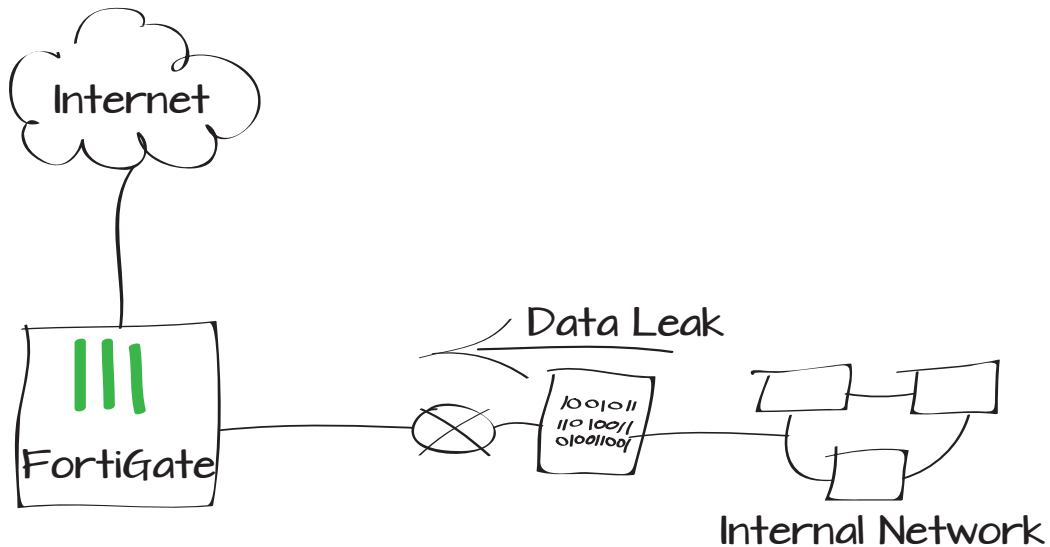
Dst	172.20.120.24	Virtual Domain	root
Protocol Number	6	Severity	critical
Service	http	Protocol	tcp
Identity Index	0	Message	anomaly: tcp_syn_flood, 21 > threshold 20, repeats 4 times
Dst Port	80	Reference	http://www.fortinet.com/ids/VID100663396
roll	65522	Status	clear_session
Timestamp	Wed Apr 24 16:04:33 2013	Sequence Number	0
Policy ID	0	Src Interface	wan1
Src	172.20.120.123	Count	4
Level	alert	Sensor	DoS-policy1
pcap_id	100663396	Src Port	62132
Log ID	18432	Sub Type	anomaly
Attack ID	100663396	Attack Name	tcp_syn_flood
Date/Time	04-24 16:04 (Wed Apr 24 16:04:33 2013)		



# Blocking outgoing traffic containing sensitive data

Data leak prevention (DLP) analyzes outgoing traffic and blocks any sensitive information from leaving the network. In this example, DLP will be used to block files using the file's name and type.

1. Creating a file filter
2. Creating a DLP sensor that uses the file filter
3. Adding the DLP sensor to a security policy
4. Results



# Creating a file filter

Go to **Security Profiles > Data Leak Prevention > File Filter**. Select **Create New** to make a File Filter Table.

Create a new filter in the table. Set the **Filter Type** to **File Name Pattern** and enter the pattern you wish to match. If needed, you can use a wildcard character in the pattern.

Create a second filter, this time setting the **Filter Type** to **File Type**. Select a **File Type** from the list.

Name	WLAN
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	10.10.10.1/255.255.255.0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access

New Filter

Filter Type

☒ File Name Pattern ☐ File Type

File Name Pattern

Security\*.pdf

OK

Cancel

New Filter

Filter Type

☐ File Name Pattern ☒ File Type

File Type

Executable (exe)

OK

Cancel

# Creating a DLP sensor that uses the file filter

Go to **Security Profiles > Data Leak Prevention > Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.

Select **Create New** to make a new filter. Set the type to **Files**. Enable **File Type included in** and set it to your file filter.

Under **Examine the following Services**, select the services you wish to monitor with DLP.

Set the **Action** to **Block**.

New Sensor

Name:My\_custom\_sensor

Comment:Comment0/255

Create New

Edit Filter

Delete

Seq #	Type	Action	Services	Archive
No matching entries found				

Filter

Messages

Files

Containing

Credit Card #

File Size >=

kB

File Type included in

My\_custom\_file\_name\_patterns

File Finger Print

Critical

Watermark Sensitivity:

Critical

Corporate Identifier:

Regular Expression

Encrypted

Examine the following Services

☒SMTP

☒IMAP

☒FTP

☒ICQ

☒Yahoo!

☒MAPI

☒POP3

☒HTTP

☒AIM

☒MSN

☒NNTP

Action

Block

## Adding the DLP sensor to a security policy

Go to **Policy > Policy > Policy**. Edit the security policy that controls the traffic you wish to block.

Enable **DLP Sensor** and set it to use the new sensor.

Policy Type: ☒ Firewall ☐ VPN

Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface:

Source Address:

Outgoing Interface:

Destination Address:

Schedule:

Service:

Action:

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Click to add...

**Logging Options**

☐ No Log

☐ Log UTM Events

☒ Log all Sessions

**Security Profiles**

AntiVirus

Web Filter

Application Control

IPS

Email Filter

DLP Sensor





## Results

Attempt to upload a file that matches the file filter criteria using FTP protocol. The file should be blocked and a message from the server should appear.



To find more information about the blocked traffic, go to **Log & Report > Traffic Log > Forward Traffic**.

The selected log message shows the name of the file that was blocked (File\_pattern\_text.exe), the type of file filter that blocked it (file-type), and a variety of other information which may be useful.

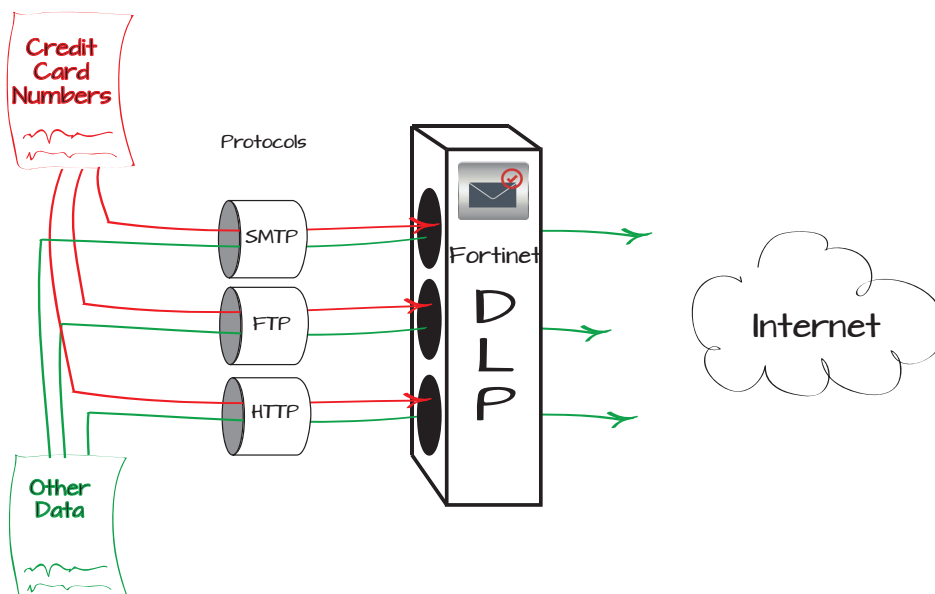
Dst	 66.11.146.80	Virtual Domain	root
Received	3481	Source Country	Reserved
UTM Action		Src NAT IP	172.20.120.23
Sent / Received	2.96 KB / 3.40 KB	Duration	11
Sent	3035	Src NAT Port	49845
Application Details		Service	HTTP
Protocol	6	Destination Country	Canada
File Name	Security Document #1.pdf	Dst Port	80
roll	65507	Status	close
UTM Sub Type	file-type	Timestamp	Mon Apr 15 12:15:28 2013
Tran Display	snat	Sequence Number	21641
Policy ID	1	Src Interface	lan
Src	192.168.1.111	UTM Event	dlp
DLP Rule Index	4	Sent Packets	8
Level	notice 	Src Port	49845
Log ID	13	Sub Type	forward
Threat	 file-type	Received Packets	6
Date/Time	12:15:28 (Mon Apr 15 12:15:28 2013)	Hostname	careers2.hiredesk.net
Dst Interface	wan1		

# Preventing credit card numbers from escaping your network

The following recipe describes how to configure your FortiGate to use DLP (Data Loss Prevention) so that credit card numbers cannot be sent out of your network using FTP, SMTP email, or by posting to a webpage.

Consumer transactions over the Internet is based upon the idea that the consumer trusts the vendor not to allow their credit card number into the possession of any unintended persons. If you deal with anyone's credit cards you may be legally responsible for their security. Having the firewall prevent their loss through digital channels may give both you and your customers some added piece of mind.

1. Obtaining credit card numbers for testing
2. Creating the DLP profile
3. Configuring the Proxy Options
4. Configuring the firewall policy
5. Results



# Obtaining credit card numbers for testing

In order to test the validity of the profile you will need to use a credit card number in the traffic. A test number (will not work for purchasing) can be obtained from one of these pages:

[http://www.paypalobjects.com/en\\_US/vhelp/paypalmanager\\_help/credit\\_card\\_numbers.htm](http://www.paypalobjects.com/en_US/vhelp/paypalmanager_help/credit_card_numbers.htm)

<http://www.crazysquirrel.com/finance/test-cc.aspx>

<http://www.getcreditcardnumbers.com/>

Create a text file that contains some of these sample credit card numbers.

# Creating the DLP Profile

## Creating the Sensor

Go to **Security Profiles > Data Leak Prevention > Sensors**.

getCreditCardNumbers

HomeCredit CardsGeneratorCVV NumbersGlossaryValidator

# Get Credit Card Numbers

Valid Credit Card Numbers for Testing Purposes!

ANDROID APP ON Google play

Visa	Mastercard	Discover	American Express
4485792214509869	5208412646419461	6011519999103396	347511708311186
4532701741207056	5325893226151723	6011531760832020	375568628598248
4539024689546572	5204853620533922	6011524935875073	372889806672016
4916224787780866	5163731025393713	6011475676000605	346925725836135
4485967693969343	5531889234744046	6011162656896208	348314150332886

(THESE CREDIT CARD NUMBERS ARE AUTOMATICALLY GENERATED EVERY TIME YOU RELOAD)

Edit Sensor default

Name: default

Comment: summary archive email and web traffic 37/255

Create NewEdit FilterDelete

Seq #	Type	Action	Services	Archive
No matching entries found				

Apply

Create a new profile by either selecting the **Create New** icon or the **View List** icon. If using the **View List** option you will then need to select the **Create New** option from the menu bar in the next window.

Once the **New Sensor Window** is open, type into the **Name** field whatever name you want for the the name of the profile.

### Creating Filters

Use the **Create New** option to create new individual filters.

For the first sensor, choose the **Messages** filter type, set it to messages **Containing Credit Card #**, select the services you wish to examine, and set **Action** to **Block**.



**New Sensor**

Name:

Comment:  0/255

[+ Create New](#) [Edit Filter](#) [Delete](#)

Seq #	Type	Action	Services	Archive
No matching entries found				

**New Filter**

**Filter**

☒ Messages ☐ Files

☒ Containing

☐ Regular Expression

**Examine the Following Services**

Web Access ☒ HTTP-POST

Email ☒ SMTP ☒ POP3 ☒ IMAP ☐ MAPI

Others ☐ NNTP

**Action**



For the second filter choose the **Files** filter type set it to messages **Containing Credit Card #**, select the services you wish to examine, and set **Action** to **Block**.



In this case we are going to choose both HTTP-POST and HTTP-GET. This will prevent not only the posting of credit card information to a web page, but the downloading of them as well.

Check the listing of the filters in the sensor to make sure that the correct protocols are selected and the action in each is set to **Block**.

## Configuring the Proxy Options

Protocols don't always use the standard ports, so proxy options will be configured to scan any port that is carrying traffic from the targeted protocol.

New Filter

Filter

Messages

Files

Containing

Credit Card #

File Size >=

KB

File Type included in

builtin-patterns

File Finger Print

Critical

Watermark Sensitivity:

Critical

Corporate Identifier:

Regular Expression

Encrypted

Examine the Following Services

Web Access

HTTP-POST

HTTP-GET

Email

SMTP

POP3

IMAP

MAPI

Others

FTP

NNTP

Action

Block

OK

Cancel

Name:

Company\_Credit\_Card\_Profile

Comment:

Comment

0/255

Create New

Edit Filter

Delete

Seq...	Type	Action	Services	Archive
1	Containing Credit Card	Block	SMTP, POP3, IMAP, HTTP-POST	Disable
2	Containing Credit Card	Block	SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP	Disable

Apply

Go to **Policy > Policy > Proxy Options**.

Create a new Proxy Option profile.

In the **Protocol Port Mapping** section change the inspection ports from **Specify** to **Any** for the protocols **HTTP, SMTP, and FTP**.

In the other option areas, select options that match up with the normal settings used by your organization.

New Proxy Options

Name

DLP\_Proxy\_Options

Comments

Write a comment...

0/255

Protocol Port Mapping

Enable	Protocol	Inspection Port(s)	
<input checked="" type="checkbox"/>	HTTP	<input checked="" type="radio"/> Any <input type="radio"/> Specify	80
<input checked="" type="checkbox"/>	SMTP	<input checked="" type="radio"/> Any <input type="radio"/> Specify	25
<input checked="" type="checkbox"/>	POP3	<input type="radio"/> Any <input checked="" type="radio"/> Specify	110
<input checked="" type="checkbox"/>	IMAP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	143
<input checked="" type="checkbox"/>	FTP	<input checked="" type="radio"/> Any <input type="radio"/> Specify	21
<input checked="" type="checkbox"/>	NNTP	<input type="radio"/> Any <input checked="" type="radio"/> Specify	119
<input checked="" type="checkbox"/>	MAPI	135	
<input checked="" type="checkbox"/>	DNS	53	
<input checked="" type="checkbox"/>	IM	<input checked="" type="radio"/> Any	

Common Options

Comfort Clients

☐

Block Oversized File/Email

☐

Web Options

Enable Chunked Bypass

☐

Add Fortinet Bar

☐

Email Options

Allow Fragmented Messages

☐

Append Signature (SMTP)

☐

OK

Cancel

# Configuring the Firewall Policy

Go to **Policy > Policy > Policy**.

As this policy is designed to prevent specific information from leaving the network the direction of the policy is from the internal interface, in this case LAN, to the external interface, wan1.

In the **Security Profiles** section, enable the **DLP Sensor** and choose the sensor created for blocking the credit card numbers as well as the appropriate Proxy Option profile.



You can also include the use of **SSL/SSH Inspection** if you have that configured to your satisfaction. This will help prevent loss of data through SSL connections.

New Policy

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

LAN

Source Address

LAN\_Addresses

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Logging Options

☐ No Log

☒ Log Security Events

☐ Log all Sessions

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

OFF

IPS

default

OFF

Email Filter

default

ON

DLP Sensor

Company\_Credit\_Card\_Profile

Proxy Options

DLP\_Proxy\_Options

ON

SSL/SSH Inspection

default

☐ Traffic Shaping

☐ Disclaimer

Comments

Write a comment...

0/1023

OK

Cancel

# Results

## Testing SMTP

Using your favorite email client, send a control email to an email server on the other side of the FortiGate unit to verify everything is working. Then try sending two emails; one with the credit card numbers in the body of the email message and one with the text document as an attachment.

The control email makes it through, but the emails with the credit card information are not received at their destination.

Go to **Log & Report > Traffic Log > Forward Traffic**. You should be able to find a log entries showing that the traffic was blocked. The logs even states that the reason they were considered threats had to do with **credit-card** information.



Because secure SMTP may not use port 25, don't filter too narrowly when searching the logs.

Also depending on your logging configuration, the logs may not show up in real-time.

Refresh		Download Raw Log		Log location: FortiAnalyzer			
#	Date/Time	Source	Dev...	Destination	Application Name	Security Acti...	Sen
1	02-03 15:37	192.168.100.100		@192.168.100.100 (unknown)	Unknown		3.00
1 / 10 [ Total: 500 ]							
Application Details				DLP Rule Index 1			
DLP Sensor		Company_Credit_Card_Profile		Date/Time		02-03 15:37 (1391441832)	
Destination		@192.168.100.100 (unknown)		Destination Country		Canada	
Dst Interface		wan1		Dst Port		587	
Duration		13		Level		notice	
Log ID		13		Mail Count		1	
Policy ID		5		Protocol		6	
Received		5068		Received Packets		34	
Recipient		@fortinet.com		Security Action			
Security Event		dip		Security Sub Type		credit-card	
Sender		@example.com		Sent		3072	
Sent / Received		3.00 KB / 4.95 KB		Sent Packets		35	
Sequence Number		872185		Service		587/tcp	
Source		192.168.100.100		Source Country		Reserved	
Spam Count		0		Src Interface		LAN	
Src NAT IP		172.20.120.67		Src NAT Port		38492	
Src Port		38492		Status		close	
Sub Type		forward		Threat		credit-card	
Timestamp		Mon Feb 3 15:37:12 2014		Tran Display		snat	
Virtual Domain		root					

---

## Testing FTP

Using your preferred FTP client, upload a control file that shouldn't be stopped to an FTP server on the other side of the FortiGate unit.

To be as generic as possible, this example uses the command line.

```
ftp ftp.example.com 1121
Connected to ftp.example.com.
220 (vsFTPd 2.3.5)
Name (ftp.example.com:): talesian
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode
(|||61875|).
150 Here comes the directory listing.
    <Various files and directories>
226 Directory send OK.
ftp> put /<path to file's directory>/DLP_
test_file.doc DLP_test_file.doc
local: /<path to file's directory>/DLP_test_
file.doc remote: DLP_test_file.doc
229 Entering Extended Passive Mode
(|||61874|).
150 Ok to send data.
100% |*****
*****| 27136
580.79 KiB/s    00:00 ETA
226 Transfer complete.
27136 bytes sent in 00:00 (130.76 KiB/s)
ftp>
```

Once you have verified that your FTP session is working properly, try to upload the text file with the credit card numbers to the FTP server.

Using the command line, everything progresses the same as the previous example until after the “put” command has been entered. At this point there is a delay while the client tries to upload the file. After a number of attempts the client gives up.

GUI FTP clients will show that it cannot proceed past the queueing process. Depending on the client, the connection to the FTP server will time out waiting for the upload to occur.

## Testing HTTP

HTTP can be tested in two directions; posting a credit card number and getting a credit card number.

Try visiting one of the sites that you received the test credit card number from. You will receive a replacement message about the transfer.

```
229 Entering Extended Passive Mode  
(|||61879|).
```

```
Abort trap: 6  
<local system prompt>$
```

### Attention!!

The transfer attempted appeared to contain a data leak!

URL = [www.paypalobjects.com/en\\_US/vhelp/paypalmanager\\_help/credit\\_card\\_numbers.htm](http://www.paypalobjects.com/en_US/vhelp/paypalmanager_help/credit_card_numbers.htm)

To test posting a credit card number, go to a site on the far side of the firewall that you can edit. In this example, a wiki test page was started on a remote site and the test credit card numbers were entered in to the page. They were allowed onto the editing screen because that was on the local computer's browser.

The content is not actually sent over the network until the **Save page** button is selected. At this point a warning message is displayed to indicate that the transfer appeared to contain a data leak.




## Creating test

[Special:Badtitle](#) > [Special:UserLogin](#) > [Main Page](#) > [Special:Search](#) > [test](#)

You have followed a link to a page that does not exist yet. To create the page, start typing in the box below (see the [help page](#) for more info). If you are here by mistake, click your browser's **back** button.

Wikikitext

PreviewChanges

**B** **I**    [Advanced](#) [Special characters](#) [Help](#)

Credit Card Numbers

Visa

- 4556851486440205
- 4024007129405931
- 4929032067481401
- 4929456698984980
- 4556627900660457

Mastercard

- 5291605760865447
- 5239105553689406
- 5152467716683681

Summary:

☐ Watch this page

Please note that all contributions to TAC Wiki may be edited, altered, or removed by other contributors. If you do not want your writing to be edited mercilessly, then do not submit it here.

You are also promising us that you wrote this yourself, or copied it from a public domain or similar free resource (see [TAC Wiki:Copyrights](#) for details). **Do not submit copyrighted work without permission!**

Save page

Show preview

Show changes

Cancel | [Editing help](#) (opens in new window)

### Attention!!

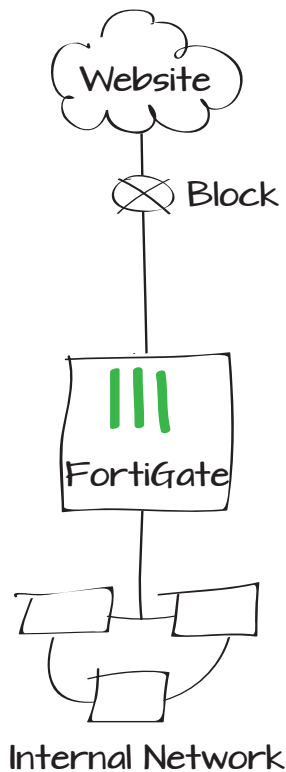
The transfer attempted appeared to contain a data leak!

URL = forti[REDACTED]/index.php?title=test&action=submit

# Blocking access to specific websites

This example sets up the FortiGate unit to block users from viewing a specific website using web filtering.

1. Creating a web filter profile
2. Adding the web filter profile to a security policy
3. Results





# Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**.

Create a new profile and select **Enable Web Site Filter** and **Create New**. Set the **URL** to \*fortinet.com, using \* as a wildcard character in order to block all subdomains of the site. Set the **Type** to **Wildcard** and the **Action** to **Block**.

# Adding the web filter profile to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling the traffic you wish to block from the website. Under **Security Profiles**, enable **Web Filter** and set it to use the new profile.

☒ Enable Web Site Filter

Create New

Edit

Delete

URL	Type	Action	Status
*fortinet.com	Wildcard	Block	Enable

Advanced Filter

OK

Cancel

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

all

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Security Profiles

OFF AntiVirus

ON Web Filter

default

My\_Web\_Filter\_Profile

## Results

In a web browser, visit [www.fortinet.com](http://www.fortinet.com) and [docs.fortinet.com](http://docs.fortinet.com). In both cases, the FortiGate unit displays a message, stating that the website is blocked.



This example will only block HTTP web traffic. In order to block HTTPS traffic as well, see “Blocking HTTP and HTTPS traffic with web filtering” on page 164.

### The URL you requested has been blocked

The page you have requested has been [blocked](#), because the URL is banned.

URL = [fortinet.com/](http://fortinet.com/)

### The URL you requested has been blocked

The page you have requested has been blocked, because the URL is [banned](#).

URL = [docs.fortinet.com/fgt.html](http://docs.fortinet.com/fgt.html)

# Extra help: Web filtering

This section contains tips to help you with some common challenges of FortiGate web filtering.

The Web Filter option does not appear in the GUI.

Go to **Config > System > Features** and enable **Web Filter**.

New Web Filter profiles cannot be created.

Go to **Config > System > Features** and select **Show More**. Enable **Multiple Security Profiles**.

Web Filtering has been configured but is not working.

Make sure that web filtering is enabled in a policy. If it is enabled, check that the policy is the policy being used for the correct traffic. Also check that the policy is getting traffic by going to the policy list and adding the Sessions column to the list.

An active FortiGuard Web Filtering license displays as expired/unreachable.

First, ensure that web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

If web filtering is enabled in a policy, go to **System > Config > FortiGuard** and click the blue arrow beside **Web Filtering**. Under Port Selection, select **Use Alternate Port (8888)**. Select **Apply** to save the changes. Check whether the license is shown as active. If it is still inactive/expired, switch back to the default port and check again.

Websites blocked using the FortiGuard Categories are not consistently blocked (for example, traffic is only blocked using certain browsers).

In your web filter profile, make sure that **Scan Encrypted Connections** is selected. Next, create an SSL Inspection profile and add it to the security policy. Traffic should now be blocked consistently.

SSL Inspection is causing certificate errors.

Download the Fortinet\_CA\_SSLProxy certificate and install it on your web browser. For more information, see [“Preventing security certificate warnings when using SSL inspection” on page 290](#).

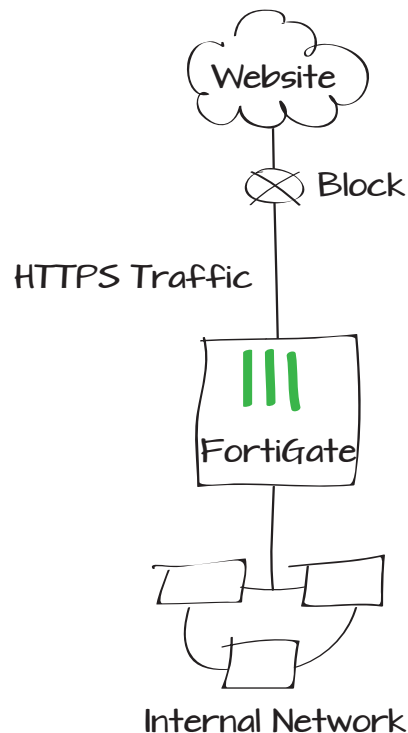
# Blocking HTTP and HTTPS traffic with web filtering

In this example, sites for streaming media will be blocked using web filtering. In order to prevent access to these sites at all times, both HTTP and HTTPS protocols must be blocked.



This example requires an active license for FortiGuard Web Filtering Services.

1. Verifying FortiGuard services are enabled
2. Creating a web filter profile
3. Creating an SSL inspection profile
4. Adding the profiles to a security policy
5. Results



## Verifying FortiGuard Services are enabled

Go to **System > Dashboard > Status**.

In the **License Information** widget, verify that you have an active subscription to FortiGuard Web Filtering. If you have a subscription, the service will have a green checkmark beside it.

License Information		
Support Contract		
Registration	Registered (Login: vancouver_support@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2014-02-25)	✓
Firmware	8 x 5 support (Expires: 2014-02-25)	✓
Enhanced Support	24 x 7 support (Expires: 2014-02-25)	✓
Comprehensive Support	24 x 7 support (Expires: 2014-02-25)	✓
FortiGuard Services		
Next Generation Firewall		
IPS & Application Control	Licensed (Expires 2014-02-25)	✓
ATP Services		
AntiVirus	Licensed (Expires 2014-02-25)	✓
Web Filtering	Licensed (Expires 2014-02-24)	✓
Other Services		
Vulnerability Scan	Licensed (Expires 2014-02-25)	✓
Email Filtering	Licensed (Expires 2014-02-24)	✓

## Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**. Select the plus icon in the upper right corner to create a new profile.

Enable **FortiGuard Categories** and expand the category **Bandwidth Consuming**. Right-click on **Streaming Media and Download**, the category to which Youtube belongs, and select **Block**.

Name

Comments

Inspection Mode ☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All

- ☒ Potentially Liable
- ☒ Adult/Mature Content
- ☒ Bandwidth Consuming
  - ☒ Freeware and Software Downloads
  - ☒ File Sharing and Storage
  - ☒ Streaming Media and Download
  - ☒ Peer-to-peer File Sharing
  - ☒ Internet Radio and TV
  - ☒ Internet Telephony
- ☒ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business

## Creating an SSL inspection profile

Go to **Policy > Policy > SSL Inspection**.  
Select the plus icon in the upper right corner  
to create a new profile.

**Enable** the inspection of the HTTPS Protocol.

Name

block\_https

Comments

Write a comment...

0/255

SSL Inspection Options

CA Certificate

Fortinet\_CA\_SSLProxy

Inspect All Ports

☐

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	443
<input type="checkbox"/>	SMTPS	465
<input type="checkbox"/>	POP3S	995
<input type="checkbox"/>	IMAPS	993
<input type="checkbox"/>	FTPS	990

# Adding the profiles to a security policy

Go to **Policy > Policy > Policy**.

Edit the security policy controlling the traffic you wish to block. Under **Security Profiles**, enable **Web Filter** and **SSL Inspection** and set both to use the new profiles.


Policy Type

☒ Firewall ☐ VPN



Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity


Incoming Interface

internal 



Source Address

 all 



Outgoing Interface

wan1 



Destination Address

 all 



Schedule

 always 

Service

 ALL 

Action

 ACCEPT 

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Click to add...

Logging Options


☐ No Log

☐ Log Security Events



☒ Log all Sessions

Security Profiles


AntiVirus

default 


Web Filter

Block\_https  


Application Control

default 


IPS

default 


Email Filter

default 


DLP Sensor

default 



VoIP

default 



ICAP

default 

Proxy Options

default  

SSL Inspection

Block\_https  

# Results

Browse to <https://www.youtube.com>. A replacement message appears indicating that the website was blocked.

Blocked traffic can be monitored by going to **Security Profiles > Monitor > Web Monitor**.





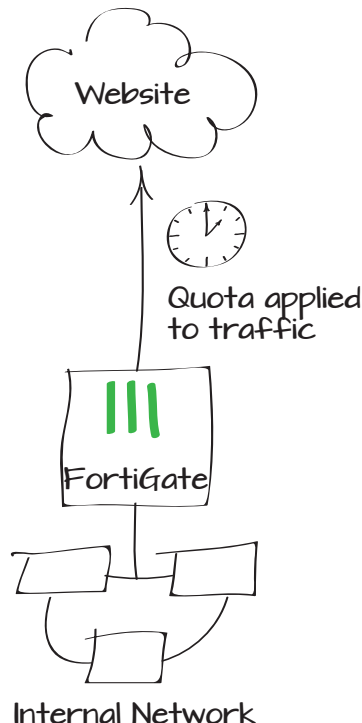
# Limiting access to personal interest websites using quotas

Many workplaces allow employees to access personal interest websites during their breaks. The most efficient method to do this is by using quotas, since they do not require set schedules. This example uses quotas to allow access at any point during the day but only for a total of 15 minutes for each user.



This example requires an active license for FortiGuard Web Filtering Services.

1. Creating a web filter profile that uses quotas
2. Adding the web filter profile to a security policy
3. Adding HTTPS scanning (optional)
4. Results



## Creating a web filter profile that uses quotas

Go to **Security Profiles > Web Filter > Profiles**.

Create a new profile and enable **FortiGuard Categories**. Right-click on the category **General Interest - Personal** and select **Monitor**. Do the same for the category **General Interest - Business**

These categories include a variety of sites that are commonly blocked in the workplace, such as games, instant messaging, and social media.

Expand **Quota on Categories with Monitor, Warning and Authenticate Actions** and select **Create New**. Select both **General Interest - Personal** and **General Interest - Business** and set the **Quota** amount to 15 Minutes.



You can also apply quotas to specific sub-categories within a FortiGuard Category, such as Shopping and Auction and Social Networking, both of which are found in the General Interest - Personal category). By doing this, you can target specific sites you wish to limit without affecting every site within the larger category.

Name: quotas

Comments: allows access to general interest with quotas 45/255

Inspection Mode: ☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All

- ☒ Local Categories
- ☒ Potentially Liable
- ☒ Adult/Mature Content
- ☒ Bandwidth Consuming
- ☒ Security Risk
- ☒ General Interest - Personal
- ☒ General Interest - Business
- ☒ Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

☒ General Interest - Personal

☒ General Interest - Business

☒ Unrated

Quota: 15 Minute(s)

## Adding the web filter profile to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling the traffic you wish to apply the quotas to. Under **Security Profiles**, enable **Web Filter** and set it to use the new profile.

The screenshot shows the configuration page for a security policy. The left sidebar contains the following sections:

- Policy Type**: Firewall (selected), VPN
- Policy Subtype**: Address (selected), User Identity, Device Identity
- Incoming Interface**: lan
- Source Address**: all
- Outgoing Interface**: wan1
- Destination Address**: all
- Schedule**: always
- Service**: ALL
- Action**: ACCEPT
- Enable NAT**: checked
  - Use Destination Interface Address (selected)
  - Use Dynamic IP Pool
  - Use Central NAT Table
- Logging Options**
  - No Log
  - Log Security Events (selected)
  - Log all Sessions
- Security Profiles**
  - AntiVirus: OFF
  - Web Filter: ON

The right sidebar contains the following sections:

- Fixed Port**: Click to add...
- Security Profiles**
  - default
  - quotas (selected)

## Adding HTTPS scanning (optional)

If you wish to apply the quotas to HTTPS traffic as well as HTTP, you must create an SSL inspection profile and add it to your security policy. For more information about blocking HTTPS traffic, see [“Blocking HTTP and HTTPS traffic with web filtering”](#) on page 164.

# Results

Browse to [www.ebay.com](http://www.ebay.com), a website that is found within the General Interest - Personal category.

Access to the website is allowed for 15 minutes, after which a block message appears. The message will persist for all General Interest - Personal sites until the quota is reset, which occurs every day at midnight.

Go to **Log & Report > Traffic Log > Forward Traffic Log** to monitor allowed and blocked traffic to these categories that have quotas.

Select an entry for more information about a session.

FortiGuard Web Filtering

Web Page Blocked

Your daily quota for this category of webpage has expired, in accordance with your internet usage policy.  
URL: [www.ebay.com/chp/collectibles-art](http://www.ebay.com/chp/collectibles-art)  
Category: Shopping and Auction  
To have the rating of this web page re-evaluated [please click here](#).

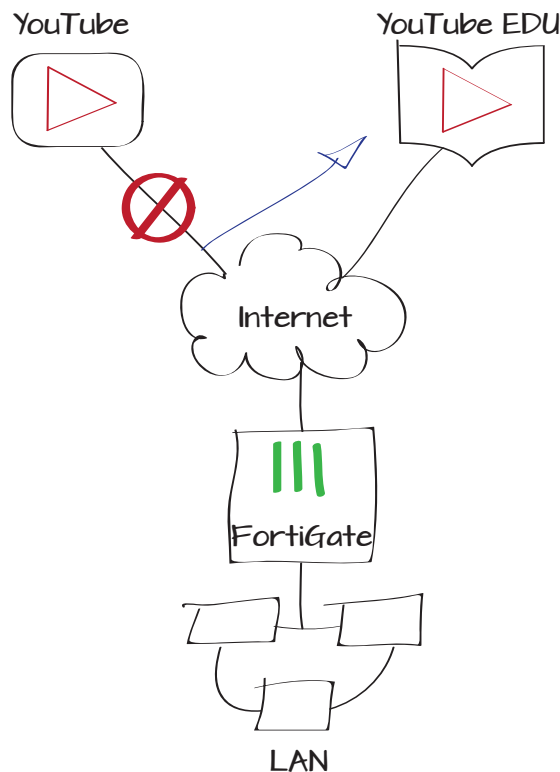
Dst	Security Acti...	Application Details	Threat
173.194.43.66 (www.google-analytics.com)		safebrowsing.clients.google.com	Search Engines and Portals
108.160.162.43 (notify5.dropbox.com)		notify5.dropbox.com	File Sharing and Storage
93.158.134.25 (mail.yandex.ru)		mail.yandex.com	Web-based Email
108.160.162.43 (notify5.dropbox.com)		notify5.dropbox.com	File Sharing and Storage
66.135.211.36 (srv.g.ebay.com)		srx.main.ebayrtm.com	Shopping and Auction
66.211.181.181 (www.ebay.com)		www.ebay.com (and another)	Shopping and Auction
174.37.236.19 (cacerts.digicert.com)		cacerts.digicert.com	Information Technology
108.160.163.51 (notify5.dropbox.com)		notify5.dropbox.com	File Sharing and Storage
132.246.2.7 (static.ak.facebook.com)			
66.211.181.181 (www.ebay.com)		www.ebay.com (and another)	Shopping and Auction

Application Details	srx.main.ebayrtm.com	Category Description	Shopping and Auction
Date/Time	07:40:56 (1378280456)	Destination Country	United States
Dst	66.135.211.36 (srv.g.ebay.com)	Dst Interface	wan1
Dst Port	80	Duration	11
Hostname	srx.main.ebayrtm.com	Level	notice
Log ID	13	Policy ID	2
Protocol	6	Received	3473
Received Packets	6	Security Action	
Security Event	webfilter	Security Sub Type	ftgd-quota
Sent	701	Sent / Received	701 B / 3.39 KB
Sent Packets	4	Sequence Number	29326
Service	HTTP	Source Country	Reserved
Src	192.168.100.112	Src Interface	lan
Src NAT IP	172.20.120.236	Src NAT Port	57344
Src Port	57344	Status	close
Sub Type	forward	Threat	Shopping and Auction
Timestamp	Wed Sep 4 07:40:56 2013	Tran Display	snat
URL Count	1	Virtual Domain	root

# Setting up YouTube for Education

This recipe describes how to apply the YouTube For Education filter, preventing access to all videos that are not part of YouTube's Education portal. It also describes how to implement security policies to prevent two common workarounds that allow users to avoid the filter: using HTTPS access, and visiting a specific YouTube URL.

1. Adding an Application Control Sensor
2. Creating URL and Category web filters
3. Configuring SSL/SSH Inspection
4. Creating blocking and redirecting security policies
5. Results



# Adding an Application Control Sensor

Go to **Security Profiles > Application Control > Application Sensors**.

Select the Plus icon in the upper right corner to create a new application sensor.

Select **Create New** to create the application filter, and set the **Sensor Type** to **Specify Applications**. Filter the results by searching for 'youtube', and highlight all the entries that contain it.

Set the **Action** to **Block**.

Sensor Type

☐ Filter Based ☒ Specify Applications

Filter Options

☒ Basic ☐ Advanced

youtube

Application Name	Category	Technology
Free.Youtube.Download	Video/Audio	Client-Server
YouTube_Video.Embedded	Video/Audio	Browser-Based
Youtube	Video/Audio	Browser-Based
Youtube.Downloader.YTD	Video/Audio	Client-Server
Youtube_Comment.Posting	Video/Audio	Browser-Based
Youtube_HD.Streaming	Video/Audio	Browser-Based
Youtube_Play.Video	Video/Audio	Browser-Based
Youtube_Search.Safety.Mode.Off	Video/Audio	Browser-Based
Youtube_Search.Video	Video/Audio	Browser-Based
Youtube_Uploading	Video/Audio	Browser-Based

Action

Monitor

Block

Reset

Traffic Shaping

# Creating URL and Category web filters

Go to **Security Profiles > Web Filter > Profiles**. You'll need to create two filters; one to block access to the YouTube URL and one to enforce the YouTube Education Filter.

Create a new web filter profile, that will block HTTP and HTTPS access to YouTube.

Enable **Web Site Filter**, and create a new URL filter, entering “\*.youtube.com” as the URL. Set the Type to **Wildcard**, and the **Action** to **Block**.

Name

Block\_YouTube\_HTTPS

Comments

Write a comment... 0/255

Inspection Mode

☒ Proxy ☐ Flow-based ☐ DNS

☐ FortiGuard Categories

Show All X

Local Categories

Potentially Liable

Adult/Mature Content

Bandwidth Consuming

Security Risk

General Interest - Personal

General Interest - Business

Unrated

Quota on Categories with Monitor, Warning and Authenticate Actions

☐ Enable Safe Search

☒ Scan Encrypted Connections (Exempted Categories: ☒ Banking ☒ Health Care ☒ Personal Privacy )

☒ Enable Web Site Filter

Create New Edit Delete

URL	Type	Action	Status
*.youtube.com	Wildcard	Block	Enable

Create a second web filter profile, that will enforce the YouTube for Education filter.

You can also enable FortiGuard Categories to block other unwanted content, but **Bandwidth Consuming > Streaming Media and Download** must be allowed or your users will not be able to access the Education portal.

Enable **Safe Search**, and enable the **Youtube Education Filter**. Enter the Education Filter registration code, provided to you by YouTube. To get a code, visit <http://www.youtube.com/t/education>.

# Configuring SSL/SSH Inspection

Go to **Policy > Policy > SSL/SSH Inspection**.

Create a new **Deep Inspection Options** profile. Ensure that **SSH Deep Scan** is enabled.

Name

YT\_Education\_Filter

Comments

Write a comment...

Inspection Mode

☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show ☒ Allow

Bandwidth Consuming

- ☐ File Sharing and Storage
- ☐ Freeware and Software Downloads
- ☐ Internet Radio and TV
- ☐ Internet Telephony
- ☐ Peer-to-peer File Sharing
- ☒ Streaming Media and Download

☐ Quota on Categories with Monitor, Warning and Authenticate Actions

☒ Enable Safe Search

☐ Search Engine Safe Search - Google, Yahoo!, Bing, Yandex

☒ YouTube Education Filter \*\*\*\*\*

Name

YT\_Deep\_Inspection

Comments

Write a comment...

**SSL Inspection Options**

CA Certificate

Fortinet\_CA\_SSLProxy

Inspect All Ports

☐

Enable	Protocol	Inspection Port(s)
<input checked="" type="checkbox"/>	HTTPS	443
<input checked="" type="checkbox"/>	SMTPS	465
<input checked="" type="checkbox"/>	POP3S	995
<input checked="" type="checkbox"/>	IMAPS	993
<input checked="" type="checkbox"/>	FTPS	990

**SSH Inspection Options**

Enable SSH Deep Scan

☒

# Creating blocking and redirecting security policies

Now, go to **Policy > Policy > Policy**. You will need to create two policies, to prevent the two filter workarounds.

Create the first policy, which will block HTTPS traffic to YouTube.

Set the internal-network-facing interface as **Incoming Interface**, your Internet-facing interface as **Outgoing Interface**, and select HTTPS for **Service**.

Enable NAT.

Under **Security Profiles**, enable **Web Filter**, using your HTTPS filter. Enable **Application Control**, using your App filter.

Lastly, enable **SSL/SSH Inspection**, using your Deep Inspection filter.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

port1 (Internal)

all

wan1

all

always

HTTPS

ACCEPT

Security Profiles

OFF

AntiVirus

ON

Web Filter

ON

Application Control

OFF

IPS

OFF

Email Filter

OFF

DLP Sensor

OFF

VoIP

OFF

ICAP

Proxy Options

ON

SSL/SSH Inspection

default

Block\_YouTube\_HTTPS

Block\_YouTube\_App

default

default

default

default

default

default

YT\_Deep\_Inspection



Create the second policy, which will force all remaining YouTube traffic to the Education portal.

Set the internal interface as **Incoming**, the internet-facing interface as **Outgoing**, and enable NAT.

Under **Security Profiles**, enable **Web Filter**, using your Education filter.

Enable **SSL/SSH Inspection**, using your Deep Inspection filter.

Return to the policy list and move your HTTPS blocking policy as close to the top as possible without affecting existing policies.

Move the education filter policy immediately below the HTTPS policy.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

port1 (Internal)

all

wan1

all

always

ALL

ACCEPT

Security Profiles

OFF

 AntiVirus

ON

 Web Filter

OFF

 Application Control

OFF

 IPS

OFF

 Email Filter

OFF

 DLP Sensor

OFF

 VoIP

OFF

 ICAP

Proxy Options

ON

 SSL/SSH Inspection

default

YT\_Education\_Filter

default

default

default

default

default

default

default

default

YT\_Deep\_Inspection

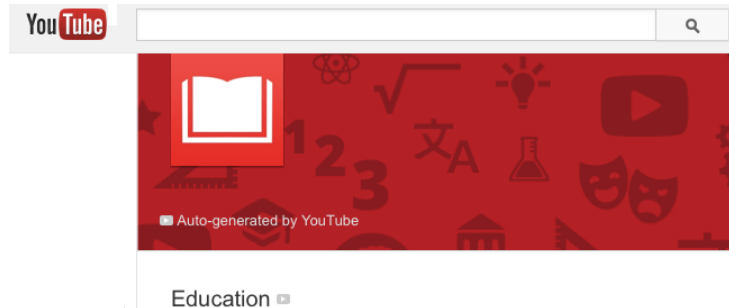
Seq.#	From	To	Service	Action	Web Filter
1	port1	wan1	HTTP HTTPS	Accept	Block_YouTube_HTTPS
2	port1	wan1	ALL	Accept	YT_Education_Filter

## Results

Browse to [www.youtube.com](http://www.youtube.com). You will arrive at the YouTube for Education homepage and only be able to access videos that have been approved as educational content.

If you attempt to avoid the filter by visiting <https://www.youtube.com>, the browser will attempt to reach the page but will eventually time out or present a message such as “The connection to the server was reset” or “Server not found”.

If you attempt to avoid the filter by visiting a specific YouTube URL, such as [www.youtube.com/watch?v=H9UtpYOwlgk](http://www.youtube.com/watch?v=H9UtpYOwlgk), the video will be replaced with an error message like the one shown.

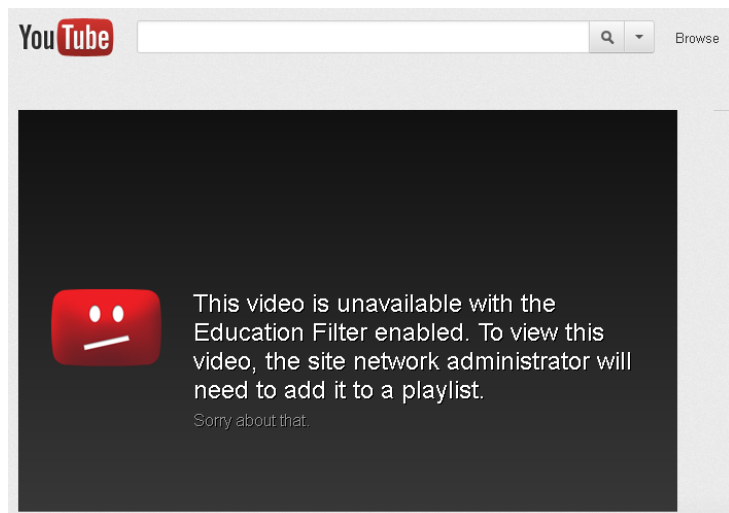


### Server not found

Firefox can't find the server at youtube.com.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again



# Using web filter overrides to control website access

This example shows two methods of using web filter overrides to control access to specific websites: one for the entire network and one for specific users.



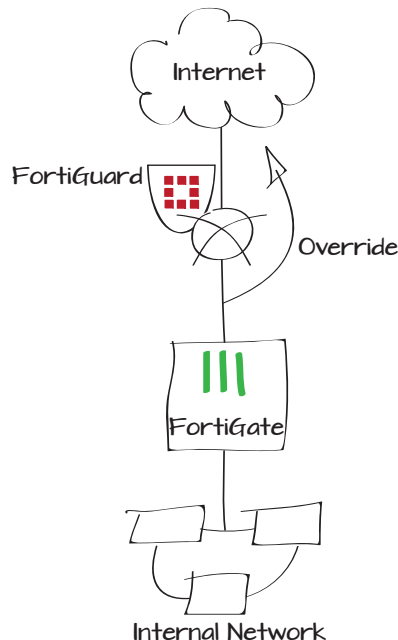
This example requires an active license for FortiGuard Web Filtering Services.

## Method 1

1. Creating a rating override
2. Adding FortiGuard blocking to the default web filter profile
3. Adding the web filter profile to a security policy
4. Results

## Method 2

1. Creating a user group and two users
2. Creating a web filter profile
3. Adding the web filter profile to a security policy
4. Results



## Method 1

### Creating a ratings override

Go to **Security Profiles > Web Filter > Rating Overrides**.

Create a new override and enter the URL `fortinet.com`. Select **Lookup Rating** to see its current FortiGuard Rating.

Set **Category** to Custom Categories (local categories) and create a new **Sub-Category** for blocked sites.

The sub-category has been added to the list of **FortiGuard Categories**, under **Local Categories**.

URL:  **Lookup Rating**

FortiGuard Rating  
Category: General Interest - Business  
Sub-Category: Information Technology

Override to  
Category:  **Custom Categories**   
Sub-Category:  **Create New**

Category Name:

**OK** **Cancel**

#### ☒ FortiGuard Categories

Show All

- ☒ Local Categories
  - ☒ blocked
  - ☒ custom1
  - ☒ custom2
- ☐ Potentially Liable
- ☐ Adult/Mature Content
- ☐ Bandwidth Consuming
- ☐ Security Risk
- ☐ General Interest - Personal
- ☐ General Interest - Business
- ☐ Unrated

## Adding FortiGuard blocking to the default web filter profile

Go to **Security Profiles > Web Filter > Profiles**.

Create a new profile and enable **FortiGuard Categories**. Right-click on **Local Categories** and select **Block**.

## Adding the web filter profile to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy that allows outbound traffic. Under **Security Profiles**, enable **Web Filter** and set it to use the new profile.

The screenshot displays the FortiGate configuration interface. The top section shows the 'block\_local' profile configuration with 'Inspection Mode' set to 'Proxy' and 'FortiGuard Categories' checked. A list of categories is shown, including 'Local Categories', 'Potentially Liable', 'Adult/Mature Content', 'Bandwidth Consuming', 'Security Risk', 'General Interest - Personal', 'General Interest - Business', and 'Unrated'. The bottom section shows the 'Policy' configuration with 'Policy Type' set to 'Firewall', 'Policy Subtype' set to 'Address', 'Incoming Interface' set to 'internal', 'Source Address' set to 'all', 'Outgoing Interface' set to 'wan1', 'Destination Address' set to 'all', 'Schedule' set to 'always', 'Service' set to 'ALL', and 'Action' set to 'ACCEPT'. The 'Enable NAT' checkbox is checked, and 'Use Destination Interface Address' is selected. The 'Logging Options' section shows 'Log Security Events' selected. The 'Security Profiles' section shows 'AntiVirus' set to 'OFF' and 'Web Filter' set to 'ON' with the 'block\_local' profile selected.

Name: block\_local  
Comments: Write a comment... 0/255  
Inspection Mode: ☒ Proxy ☐ Flow-based ☐ DNS  
☒ FortiGuard Categories  
Show: All  
+ Local Categories  
+ Potentially Liable  
+ Adult/Mature Content  
+ Bandwidth Consuming  
+ Security Risk  
+ General Interest - Personal  
+ General Interest - Business  
+ Unrated  
Quota on Categories with Monitor, Warning and Authenticate Actions

Policy Type: ☒ Firewall ☐ VPN  
Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity  
Incoming Interface: internal  
Source Address: all  
Outgoing Interface: wan1  
Destination Address: all  
Schedule: always  
Service: ALL  
Action: ACCEPT  
☒ Enable NAT  
Use Destination Interface Address ☐ Fixed Port  
Use Dynamic IP Pool Click to add...  
Logging Options  
☐ No Log  
☒ Log Security Events  
☐ Log all Sessions  
Security Profiles  
AntiVirus: OFF default  
Web Filter: ON block\_local

## Results

In a web browser, go to [www.fortinet.com](http://www.fortinet.com).

The website will be blocked and a replacement message from FortiGuard Web Filtering will appear.



Rating overrides can also be used to allow access to specific sites within a FortiGuard category, such as General Interest - Personal, while still blocking the rest of the sites listed in that category.

## Method 2

### Creating a user group and two users

Go to **User & Device > User > User Groups**. Select **Create New** and create the group *override\_group*.

The top screenshot shows the FortiGuard Web Filtering interface. It features a red 'X' icon and the title 'Web Page Blocked!'. The message states: 'You have tried to access a web page which is in violation of your internet usage policy.' Below this, it shows the URL 'www.fortinet.com/' and the category 'custom1'. There is an 'Override' link and a note: 'To have the rating of this web page re-evaluated [please click here](#).'

The bottom screenshot shows the 'Create New' user group dialog in FortiGate. The 'Name' field is set to 'override\_group'. The 'Type' is 'Firewall'. Under 'Available Users', there is a list of local users: blee, guest, jsmith, tbrown, and telbar. The 'Members' list is currently empty. There are 'OK' and 'Cancel' buttons at the bottom.

Go to **User & Device > User > User Definition.**

Using the **User Creation Wizard**, create two users (in the example, *ckent* and *bwayne*). Assign *ckent* to *override\_group* but not *bwayne*.

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

☒ Local User

☐ Remote RADIUS User

☐ Remote TACACS+ User

☐ Remote LDAP User

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

User Name

ckent

Password

\*\*\*\*\*

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

Email Address

ckent@example.com

☒ SMS

Phone Number

55555555

Service Type

FortiGuard Messaging Service

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

☒ Enable

☐ Two-factor Authentication

☒ User Group

override\_group

< Back

Done

Cancel

## Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**.

Create a new profile and enable **FortiGuard Categories**. Right click on **Local Categories** and select **Block**.

Expand the **Advanced Filter** and enable **Allow Blocked Override**. Set **Apply to Group(s)** to *override\_group*.

Set **Assign to Profile** to default to use it as the alternate web filter profile for *override\_group* users.

Because the default web filter does not block Local Categories, using it will allow cken to access fortinet.com for the duration of the override period (by default, **Duration** is set to 15 minutes).

The screenshot shows the 'Web Filter Profile' configuration page. The 'Name' field is 'override\_profile'. The 'Inspection Mode' is set to 'Proxy'. Under 'FortiGuard Categories', 'Local Categories' is expanded and 'Block' is selected. In the 'Advanced Filter' section, 'Allow Blocked Override' is checked, and 'Apply to Group(s)' is set to 'override\_group'. The 'Assign to Profile' is set to 'default'. The 'Duration' is set to 'Constant' with a value of '15' minutes. The 'Apply' button is at the bottom right.

## Adding the web filter profile to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy that allows outbound traffic and set the **Policy Subtype** to **User Identity**.

The screenshot shows the 'Policy' configuration page. The 'Policy Type' is 'Firewall'. The 'Policy Subtype' is 'User Identity'. The 'Incoming Interface' is 'internal'. The 'Source Address' is 'all'. The 'Outgoing Interface' is 'wan1'. The 'Enable NAT' checkbox is checked. The 'Apply' button is at the bottom right.



Create an **Authentication Rule** that includes both *override\_group* and *bwayne* and has **Web Filter** set to *override\_profile*.

## Results

In a web browser, go to [www.fortinet.com](http://www.fortinet.com).

After the user authentication screen, the website is blocked and a replacement message from FortiGuard Web Filtering appears.

Select **Override**. You are prompted to authenticate to view the page.

User *bwayne* is not able to override the web filter and receives an error message.

Destination Address	<input type="text" value="all"/>
Group(s)	<input type="text" value="override_group"/>
User(s)	<input type="text" value="bwayne"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input type="text" value="ACCEPT"/>

**Logging Options**

☐ No Log

☐ Log Security Events

☒ Log all Sessions

**Security Profiles**

<input type="checkbox"/> AntiVirus	<input type="text" value="default"/>
<input checked="" type="checkbox"/> Web Filter	<input type="text" value="override_profile"/>
<input type="checkbox"/> Application Control	<input type="text" value="default"/>
<input type="checkbox"/> IPS	<input type="text" value="default"/>
<input type="checkbox"/> Email Filter	<input type="text" value="default"/>
<input type="checkbox"/> DLP Sensor	<input type="text" value="default"/>



### Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: [www.fortinet.com/](http://www.fortinet.com/)  
Category: custom1

[Override](#)

To have the rating of this web page re-evaluated [please click here](#).



### Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.  
**Invalid or missing user-group id in request.**

However, user *ckent* is able to override the filter and can access the site for 15 minutes.

You can monitor web filter overrides by going to **Log & Report > Traffic Log > Forward Traffic**.

Select an entry for more information about a session, including the user and hostname.



Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.

Username:

ckent

Password:

\*\*\*\*\*

Scope:

User (ckent)

New Profile:

Web-filter Profile (default)

Duration:

0

(Days)

0

(Hours)

15

(Minutes)

Continue

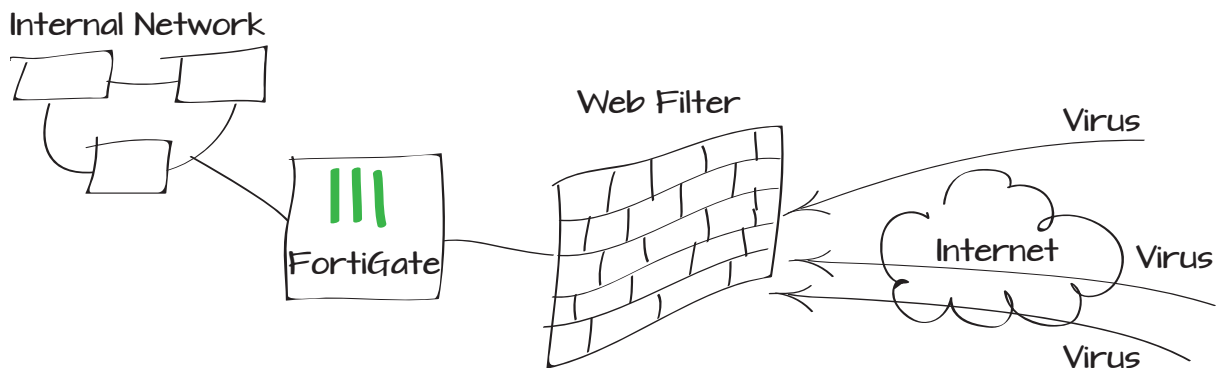
Src	Dst	Security Action	Sent / Received	Application Details
ckent (10.10.10.105)	66.171.121.34	✓	16.34 KB / 200.09 KB	www.fortinet.com (and 10 others)
ckent (10.10.10.105)	66.171.121.34	✓	15.50 KB / 117.35 KB	www.fortinet.com (and 11 others)
ckent (10.10.10.105)	66.171.121.34	✓	13.43 KB / 50.27 KB	www.fortinet.com (and 11 others)
ckent (10.10.10.105)	66.171.121.34	✓	14.36 KB / 82.41 KB	www.fortinet.com (and 11 others)
ckent (10.10.10.105)	66.171.121.34	✓	13.33 KB / 60.34 KB	www.fortinet.com (and 11 others)

Dst	66.171.121.34	Virtual Domain	root
Received	204889	Source Country	Reserved
Security Action	✓	Src NAT IP	172.20.120.126
URL Count	11	Source SSID	FortiDocs1
Duration	32	Sent	16731
Src NAT Port	62820	Application Details	www.fortinet.com (and 10 others)
Group	override_group	Service	HTTP
Protocol	6	User	ckent
Destination Country	United States	Identity Index	1
Dst Port	80	roll	0
Status	close	Security Sub Type	log-all-url
Timestamp	Tue Jun 18 07:32:38 2013	Tran Display	snat
Sequence Number	1582559	Policy ID	5
Src Interface	WLAN_1	Src	ckent (10.10.10.105)
Sent / Received	15.34 KB / 200.09 KB	Security Event	webfilter
Sent Packets	121	Level	notice
Src Port	62820	Log ID	13
Sub Type	forward	Threat	
Received Packets	160	Date/Time	07:32:38 [Tue Jun 18 07:32:38 2013]
Hostname	www.fortinet.com (and 10 others)	Dat Interface	wan1

# Inspecting traffic content using flow-based inspection

Flow-based inspection offers an alternative to proxy-based inspection, which imposes some limitations on performance and also changes some aspects of packets as they pass through your FortiGate unit. This example enables flow-based inspection for antivirus and web filtering.

1. Enabling flow-based inspection in an antivirus profile
2. Enabling flow-based inspection in a web filtering profile
3. Adding the new profiles to a security policy
4. Results



# Enabling flow-based inspection in an antivirus profile

Go to **Security Profiles > Antivirus > Profile**. Select the plus icon in the upper right corner of the window to create a new profile.

Select **Flow-based** as the **Inspection Mode**.

Configure the profile to inspect traffic based on your network needs.

Name

AV\_Flow-based

Comments

Write a comment...

0/255

Inspection Mode

☐ Proxy

☒ Flow-based

☐ Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
<b>Web</b>	
HTTP	<input checked="" type="checkbox"/>
<b>Email</b>	
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
MAPI	<input type="checkbox"/>
<b>File Transfer</b>	
FTP	<input checked="" type="checkbox"/>
SMB	<input type="checkbox"/>
<b>IM</b>	
ICQ, Yahoo, MSN Messenger	<input checked="" type="checkbox"/>

## Enabling flow-based inspection in a web filtering profile

Go to **Security Profiles > Web Filter > Profile**. Select the plus icon in the upper right corner of the window to create a new profile.

Select **Flow-based** as the **Inspection Mode**.

Configure the profile to block traffic based on your network needs.

Name

Comments  0/255

Inspection Mode ☐ Proxy ☒ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All

- ✓ Potentially Liable
- ✓ Adult/Mature Content
- ✓ Bandwidth Consuming
- ✓ Security Risk
- ✓ General Interest - Personal
- General Interest - Business
  - ✓ Finance and Banking
  - ✗ Search Engines and Portals
  - ✓ General Organizations
  - ✓ Business
  - ✓ Information and Computer Security
  - ✓ Government and Legal Organizations
  - ✓ Information Technology
  - ✓ Armed Forces
  - ✓ Web Hosting
  - ✓ Secure Websites

☐ Enable Safe Search

☐ Search Engine Safe Search - Google, Yahoo!, Bing, Yandex

## Adding the new profiles to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling the traffic you wish to inspect. Under **Security Features**, enable **Antivirus** and **Web Filter** and set them to use the new profiles.

## Results

To test the AV scanning, go to [www.eicar.org](http://www.eicar.org) and try to download a test file. The browser will time out and display a message similar to what is shown here from Google Chrome.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	internal
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
Click to add...	
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input checked="" type="radio"/> Log Security Events	
<input type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	Block_app-sensor
<input type="checkbox"/> IPS	default
<input type="checkbox"/> Email Filter	default
<input type="checkbox"/> DLP Sensor	default

## This webpage is not available

The connection to [www.eicar.org](http://www.eicar.org) was interrupted.

Here are some suggestions:

- [Reload](#) this webpage later.
- Check your Internet connection. Restart any router, modem, or other network device.
- Add Google Chrome as a permitted program in your firewall's or antivirus software program, try deleting it from the list of permitted programs and adding it again.
- If you use a proxy server, check your proxy settings or contact your network administrator to see if the proxy is working. If you don't believe you should be using a proxy server, adjust your proxy settings in **System Preferences > Network > Advanced > Proxies** and deselect any proxy servers.

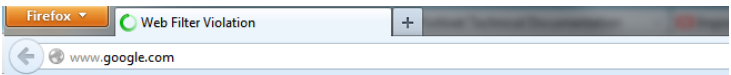
Go to **Log & Report > Traffic Log > Forward Traffic** to see the blocked traffic.

To test the web filtering, browse to [www.google.com](http://www.google.com). The FortiGate unit will display a block message.

Go to **Security Profiles > Monitor > Web Monitor** to see information about blocked Internet traffic.

Download Raw Log

me	Src	Device	Dst	Application Name	Security Action
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	

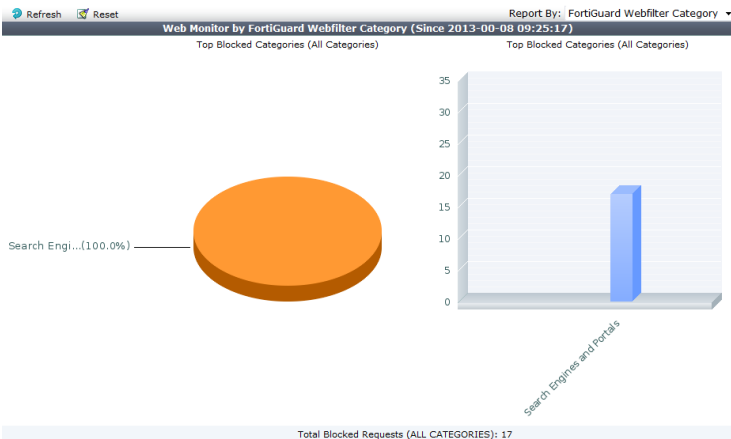


### Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: [www.google.com/](http://www.google.com/)  
Category: Search Engines and Portals

To have the rating of this web page re-evaluated [please click here](#).



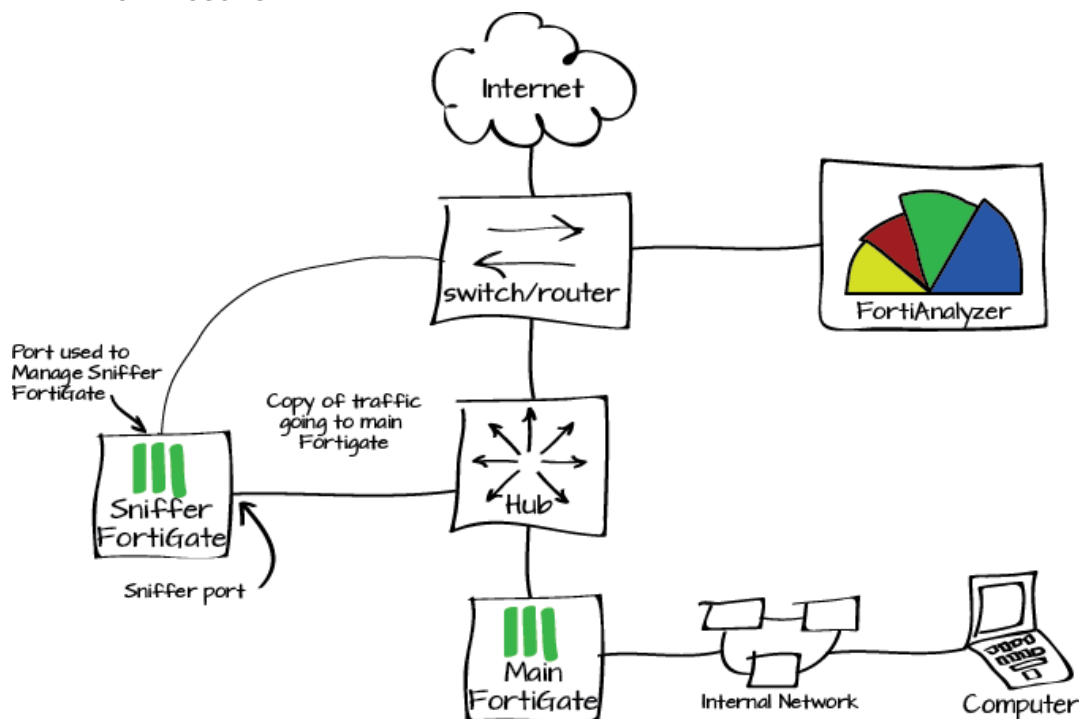
# Analyzing your network traffic using a one-armed sniffer

You can use a one-armed sniffer in coordination with a FortiAnalyzer to analyze traffic going through a main FortiGate to minimize the impact on network performance impact.

## Topology Setup

Sniffing can be done by way of port mirroring or by placing a hub between the FortiGate and the router/switch. Using a hub removes potential configuration issues with the switch.

1. Configuring the interfaces
2. Configuring the security profiles
3. Registering the sniffer device
4. Configuring logging to the FortiAnalyzer
5. Results





# Configuring the interfaces

These settings are for the FortiGate designated as the “sniffer”; in this case a FortiGate model 60D.



It is possible to use the same interface for both the mirror traffic and access to the FortiAnalyzer, but it is recommended to use one for each purpose separately.

If there is not already administratively accessible interface, consider using FortiExplorer and a USB cable.

## Configuring the Management Interface (WAN 1) on the Sniffer

Log in to the FortiGate 60D.

Go to **System > Network > Interfaces**.

Select the interface that you wish to connect to your internal network so that you can access the device remotely and allow it to connect to the FortiAnalyzer.

Verify that the configuration for the interface is completed with the information shown here. Make sure that it is on the correct subnet range.

The purpose of this interface is to manage the FortiGate and provide access to the FortiAnalyzer so it is important to make sure that the correct **Administrative Access** is chosen and that the interface is on the internal subnet.

Name	wan1(00:09:0F:B5:55:2A)
Alias	Management Port
Link Status	Up
Type	Physical Interface
Addressing mode <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP	
IP/Network Mask	172.20.120.69/255.255.255.0
IPv6 Address	:::0
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET
DHCP Server	<input type="checkbox"/> Enable
Security Mode	None
Device Management	
Detect and Identify Devices	<input type="checkbox"/>
Enable Explicit Web Proxy	<input type="checkbox"/>
Listen for RADIUS Accounting Messages	<input type="checkbox"/>
Secondary IP Address	<input type="checkbox"/>
Comments	Write a comment... 0/255
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down
<div>OK Cancel</div>	

## Configuring the sniffer interface

Select the interface that you wish to use to collect the mirrored data traffic.

Verify that the configuration for the interface is completed with the shown information:

If the One-Arm Sniffer addressing mode is unavailable you may have to choose a different interface.

## Configuring the security profiles

Some administrators match the content of the profiles on the sniffer with those on the Main FortiGate, but this is not a requirement for the sniffer to work. The sniffer profiles will not impact your network performance so they can be as comprehensive as you want. Create profiles that will capture the information you want.



If you cannot set more than one type of Security Profile go to **System > Config > Features** and ensure that the **Multiple Security Profiles** feature is enabled.

Name	wan2(00:09:0F:B5:55:2B)
Alias	Sniffer Interface
Link Status	Up
Type	Physical Interface
Addressing mode Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> <b>One-Arm Sniffer</b> <input checked="" type="radio"/> Dedicate to FortiAP <input type="radio"/>	
Enable Filters <input type="checkbox"/> <input checked="" type="checkbox"/> Include IPv6 Packets <input checked="" type="checkbox"/> Include Non-IP Packets	
<b>Security Profiles</b> <input checked="" type="checkbox"/> Enable AntiVirus Generic Flow based profile X <input checked="" type="checkbox"/> Enable Web Filter web-filter-flow X <input checked="" type="checkbox"/> Enable Application Control default X <input checked="" type="checkbox"/> Enable IPS all_default X	
Administrative Access <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request	
IPv6 Administrative Access <input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET	
Enable Explicit Web Proxy <input type="checkbox"/>	
Listen for RADIUS Accounting Messages <input type="checkbox"/>	
Secondary IP Address <input type="checkbox"/>	
Comments Write a comment... 0/255	
Administrative Status <input checked="" type="radio"/> Up <input type="radio"/> Down	
<b>OK</b> <b>Cancel</b>	

### Multiple Security Profiles ?

ON



# AntiVirus Profile (Flow-based)

Go to **Security Profiles > AntiVirus > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.



The one-armed sniffer mode will only allow flow-based profiles to be used.

Configure the following in the CLI, in addition to the web-based configuration:

Name

Generic Flow based profile

Comments

Write a comment... 0/255

Inspection Mode

☐ Proxy ☒ Flow-based

☒ Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
<b>Web</b>	
HTTP	<input checked="" type="checkbox"/>
<b>Email</b>	
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
<b>File Transfer</b>	
FTP	<input checked="" type="checkbox"/>
SMB	<input checked="" type="checkbox"/>

Apply

```
config antivirus settings
  set default-db normal
end

config antivirus profile
  edit AV-flow
    set extended-utm-log enable
    config smb
      set options scan
    end
    set av-virus-log enable
    set av-block-log enable
  end
end
```

# Application Control Sensor

Go to **Security Profiles > Application Control > Application Sensors**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.

Add the these CLI settings in addition to the web-based configuration:

Name

default

Comments

monitor all applications

24/255

☒ Allow and Log DNS Traffic

Create New

Copy

Import

Export

Reset

Category	Popularity	Technolo...	Risk	Action	Application
All + Uncommon	☆☆☆☆	All	All	Monitor	012mail,0zz0,1and1 ... <a href="#">[Show all 3118]</a>
				Monitor	All Other Known Applications
				Monitor	All Other Unknown Applications

Apply

```
config application list
  edit "default"
    set extended-utm-log enable
    set other-application-log enable
    set log enable
    set unknown-application-log enable
  end
```

## Webfilter Profile (Flow-based)

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the profile on the sniffer device as on the primary FortiGate.

The screenshot shows the configuration page for a webfilter profile named 'web-filter-flow'. The 'Name' field contains 'web-filter-flow' and the 'Comments' field contains 'flow-based web filter profile'. The 'Inspection Mode' is set to 'Flow-based' (selected with a radio button), with 'Proxy' and 'DNS' as other options. The 'FortiGuard Categories' section is checked, and a list of categories is displayed: 'Local Categories', 'Potentially Liable', 'Adult/Mature Content', 'Bandwidth Consuming', 'Security Risk', 'General Interest - Personal', 'General Interest - Business', and 'Unrated'. Below this, several checkboxes are present: 'Enable Safe Search' (unchecked), 'Scan Encrypted Connections' (checked), 'Enable Web Site Filter' (unchecked), 'Web Content Filter' (unchecked), 'Allow Websites When a Rating Error Occurs' (unchecked), and 'Rate URLs by Domain and IP Address' (unchecked). An 'Apply' button is at the bottom right.

Name: web-filter-flow

Comments: flow-based web filter profile

Inspection Mode: ☐ Proxy ☒ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All

- Local Categories
- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
- Unrated

☐ Enable Safe Search

☒ Scan Encrypted Connections

☐ Enable Web Site Filter

☐ Web Content Filter

☐ Allow Websites When a Rating Error Occurs

☐ Rate URLs by Domain and IP Address

Apply

Configure the following settings in the CLI, in addition to the web based configuration:

```
config webfilter profile
    edit web-filter-flow
        set extended-utm-log enable
        set options https-url-scan
    end
```

IPS sensor

Go to **Security Profiles > Webfilter > Profiles**.

Apply the same settings to the sensor on the sniffer device as on the primary FortiGate.

Registering the Sniffer device

Log in to the FortiAnalyzer.

Go to the **Device Manager** tab.

Select **Add Device** from the drop down menu.

In the **Login** screen of the **Add Device** wizard fill in the fields with the information shown here.

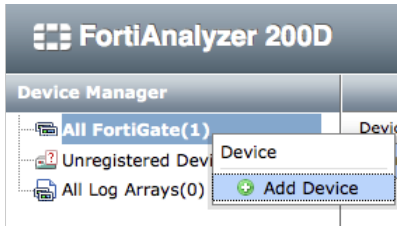
Select **Next**.

Name: all\_default

Comments: all predefined signatures with default setting 46/255

Severity	Targ...	OS	Action	Packet Logging	Matched Signatures
All	All	All	Monitor	Enable	2Wire.Wireless.Router.XSRF.Password.Reset 3Com.3CDaemon.FTP.Server.Buffer.Overflow ... [Show all 6593]

Apply



Add Device

Login

Please choose one of the following methods for adding a device or vdom.

**Add Model Device**

Device will be added using the chosen model type and other explicitly entered information.

Please enter the following information:

IP Address	172.20.120.69
User Name	admin
Password	

Next > Cancel

In the **Add Device** screen of the **Add Device** wizard fill in the fields with the information shown here.

If there is no more information to enter, select **Next**.

Select the sideways triangle next to **Other Device Information** to expand the window for more field options.

Select **Next**.

### Add Device

Please input the following information to complete addition of the device:

Name	<input type="text" value="One-Arm_Sniffer-1"/>	
Description	<input type="text" value="Sniffer_for_FG100D"/>	
Device Type	<input type="text" value="FortiGate"/>	
Device Model	<input type="text" value="FortiGate-60D"/>	
Firmware Version	<input type="text" value="5.0"/>	<input type="text" value="GA"/>
SN	<input type="text" value="FGT60D4613001043"/>	
Enable Interface Mode	<input checked="" type="checkbox"/>	
Disk Log Quota (min. 100MB)	<input type="text" value="1000"/>	MB (Total 783,298 MB Available)
When Allocated Disk Space is Full	<input checked="" type="radio"/> Overwrite Oldest Logs <input type="radio"/> Stop Logging	
Log Storage	<input checked="" type="radio"/> Standalone Logs <input type="radio"/> Log Array	
Device Permissions	<input checked="" type="checkbox"/> Logs <input checked="" type="checkbox"/> DLP Archive <input checked="" type="checkbox"/> Quarantine <input checked="" type="checkbox"/> IPS Packet Log	
▶ Other Device Information		

Device Permissions	<input checked="" type="checkbox"/> Logs <input checked="" type="checkbox"/> DLP Archive <input checked="" type="checkbox"/> Quarantine <input checked="" type="checkbox"/> IPS Packet Log
▼ Other Device Information	
Company/Organization	<input type="text" value="Daily Planet"/>
Contact	<input type="text" value="P. White"/>
City	<input type="text" value="Metropolis"/>
Province/State	<input type="text" value="DC"/>
Country	<input type="text" value="United States"/>

A window showing successful registration should appear.

Select **Next** to proceed.

The final window of the wizard provides a summary of the configuration.

### Add Device

Name	One-Arm_Sniffer-1
IP Address	172.20.120.69
Status	<div><div><div>✔</div>Device created successfully</div><div><div>✔</div>Creating device database</div><div><div>✔</div>Retrieving high availability status</div><div><div>✔</div>Initializing configuration database</div><div><div>✔</div>Updating group membership</div></div>

### Model Device Added Successfully

The following device has been added to the system:

Name	One-Arm_Sniffer-1
Description	Sniffer_for_FG100D
Hostname	N/A
IP Address	172.20.120.69
Admin User	admin
Device Model	FortiGate-60D
Firmware Version	5.0 GA
SN	FGT60D4613001043
Disk Allocation	1000 MB
Company/Organization	Daily Planet
Contact	P. White
City	Metropolis DC United States



## Configure logging to the FortiAnalyzer

Go to **Log & Filter > Log Config > Log Settings**.

Configure the settings as shown here.

Be sure to test the connectivity before proceeding.

The screenshot shows the 'Log Settings' configuration page in FortiGate. It is divided into three main sections: 'Logging and Archiving', 'Local Traffic Logging', and 'GUI Preferences'.  
**Logging and Archiving:** This section contains options for sending logs to FortiAnalyzer/FortiManager, FortiCloud, and FortiAnalyzer/FortiManager. The 'Send Logs to FortiAnalyzer/FortiManager' option is checked. The IP Address is set to 172.20.120.140, and there is a 'Test Connectivity' button. The 'Upload Option' is set to 'Realtime'. The 'Encrypt Log Transmission' option is unchecked. The 'Send Logs to FortiCloud' option is unchecked. The 'Account' field is empty, with a 'Test Connectivity' button next to it. The 'Event Logging' section has 'Event Logging' checked, and 'Enable All' is also checked. There are three columns of event types, all of which are checked: 'WiFi activity event', 'System activity event', 'User activity event', 'Router activity event', 'VPN activity event', and 'Explicit web proxy event'.  
**Local Traffic Logging:** This section has three options, all of which are checked: 'Log Allowed Traffic', 'Log Local Out Traffic', and 'Log Denied Traffic'.  
**GUI Preferences:** This section has a 'Display Logs From' dropdown menu set to 'FortiAnalyzer'. There are two checked options: 'Resolve Hostnames (Using reverse DNS lookup)' and 'Resolve Unknown Applications (Using remote application database)'. At the bottom of the page is an 'Apply' button.

## Results

### Creating some logs

On a computer behind the primary FortiGate, download some test files from the Eicar website at:

<http://www.eicar.org/85-0-Download.html>

Visit some websites that should be blocked by the policy, for example:

[www.gambling.com](http://www.gambling.com)

# Seeing the results on the FortiAnalyzer

Log in to the FortiAnalyzer

Go to the **Log View** tab.

In the left-hand column, expand the tree for the sniffer device.

Go to **Security > Intrusion Prevention**.

You will see a listing of the items that are considered relevant.

In this case the one for the test file shows the **Attack Name** as Eicar.Virus.Test.File

FortiAnalyzer 200D

Device ManagerLog ViewDrill DownEvent ManagementReportsSystem Settings

Log View

srcip=172.16.86.11 vd=vdom2

Any time

1

#		Date/Time	Severity	Source/Device	Destination IP	Status
1		02-27 11:34	low	74.217.253.60	192.168.10.103	detected
2		02-27 11:34	low	74.217.253.60	192.168.10.103	detected
3		02-27 11:34	low	173.194.43.77	192.168.10.103	detected
4		02-27 11:03	info	188.40.238.250	192.168.10.103	detected

50Items per page<<first<prev1next>>last>>Go to

Log DetailsArchive

Attack ID	29844	Attack Name	
Count	1	Date/Time	
Destination IP	192.168.10.103	Destination Name	
Destination Port	54133	Device ID	
Device Time	2014-02-27 11:03:41	Event Type	
Identity Index	0	Incident Serial No.	
Level	alert	Log ID	
Message	file_transfer: Eicar.Virus.Test.File,	Policy ID	
Protocol	6	Reference	
Sensor	all_default	Sequence No.	
Service	54133/tcp	Severity	
Source Interface	wan2	Source Port	
Source/Device	188.40.238.250	Status	
Sub Type	ips	Time Stamp	
Type	utm	Virtual Domain	

Select the **Log View** Tab.

In the left-hand column, expand the tree for the sniffer device.

Select **Traffic**.

Use the column filters to focus in on the target traffic. In this case we are looking for traffic with:

- Source IP address = 192.168.10.100
- Destination IP address = 190.93.240.30
- Service = HTTP

FortiAnalyzer 200D

Device ManagerLog ViewDrill DownEvent ManagementReportsSystem Settings

Log View

srcip=172.16.86.11 and service=HTTP

Any time

1

#	Date/Time	Policy ID	Threat	Status	Source/Device	Destination IP	Service
1	14:58:36	1		accept	192.168.10.100	190.93.240.30	HTTP
2	14:58:34	1		accept	192.168.10.100	190.93.240.30	HTTP
3	14:58:32	1		accept	192.168.10.100	190.93.240.30	HTTP
4	14:56:27	1		accept	192.168.10.100	190.93.240.30	HTTP

50Items per page<<first<prev1next>>last>>Go to page 1 of 1

Log Details

Application	HTTP.BROWSER_Firefox	Application Category	Web.Others
Application ID	34050	Date/Time	14:58:36
Destination IP	190.93.240.30	Destination Interface	N/A
Destination Port	80	Device ID	FGT6004613001043
Device Time	2014-03-31 14:58:35	Duration	0
Level	notice	Log ID	13
Policy ID	1	Protocol	6
Sent/Received	0 / 597 B	Sequence No.	7974
Service	HTTP	Source Country	Reserved
Source Interface	wan2	Source Port	12626
Source/Device	192.168.10.100	Status	accept
Sub Type	forward	Time Stamp	2014-03-31 14:58:36
Tran Display	snat	Type	traffic
Virtual Domain	root		

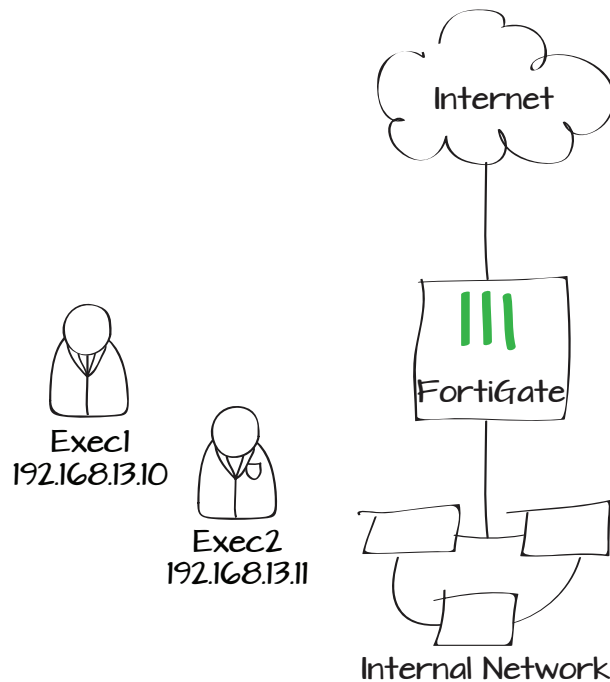


The destination address was determined by pinging gambling.com and looking at the resolved address.

# Excluding specific users from security scanning

In this example, two company executives will be excluded from the security scanning that is applied to all other Internet traffic. Since the executives connect to the Internet using the PCs that have static IP addresses, these addresses can be used to identify their traffic.

1. Applying security profiles to the staff policy
2. Creating firewall addresses and a group for the executives
3. Creating a security policy for the executives
4. Results



## Applying security profiles to the staff policy

Go to **Policy > Policy > Policy** and edit the policy allowing Internet access. This policy will be used by the majority of the company's staff.

In order to view results, select **Log all Sessions**.

Under **Security Profiles**, enable **Web Filter** and **Application Control**. Set them to use the **default** profiles.

Policy Type: ☒ Firewall ☐ VPN

Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface:

Source Address:

Outgoing Interface:

Destination Address:

Schedule:

Service:

Action:

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

**Logging Options**

☐ No Log

☐ Log Security Events

☒ Log all Sessions

☐ Capture Packets

**Security Profiles**

## Creating firewall addresses and a group for the executives

Go to **Firewall Objects > Address > Addresses**. Create an address for each executive.

Set **Type** to **Subnet** and **Interface** to **lan**. Set **Subnet/IP Range** to the static IP of the executive's PC. Use /32 as the Netmask to ensure that the firewall address applies only to the specified IP.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name:

Type:

Subnet / IP Range:

Interface:

Go to **Firewall Objects > Address > Groups**.

Create a new group and add the new addresses as members.

# Creating a security policy for the executives

Go to **Policy > Policy > Policy**.

Create a policy allowing the executives to access the Internet. Set **Incoming Interface** to **lan**, **Source Address** to the firewall address group, and **Outgoing Interface** to your Internet-facing interface. **Enable NAT** and, in order to view results, select **Log all Sessions**.

Leave all **Security Profiles** disabled.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Exec2

Type

Subnet

Subnet / IP Range

192.168.13.11/32

Interface

lan

Group Name

Executives

Comments

Write a comment... 0/255

Show in Address List

☒

Members

Exec1

Exec2

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

lan

Source Address

Executives

Outgoing Interface

wan1

Destination Address

all

Schedule

all ways

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

☐ Capture Packets

Security Profiles

OFF

AntiVirus

default

OFF

Web Filter

default

OFF

Application Control

default

In the policy list, reorder the security policies by clicking and dragging the **Seq.#** column. Place the policy for the executives at the top of the list.

## Results

Connect to the Internet from two computers on the internal network: one that has an IP address assigned to one of the executives and one that doesn't.

Go to **Log & Report > Traffic Log > Forward Traffic Log**. Right-click on one of the column headings and make sure that the **Policy ID** column is selected, then select **Apply**.

Policy IDs are assigned by the order in which policies were created and so in the example the staff policy's ID is 2, while the executive policy's ID is 3.

In the log, you can see that traffic from the computer with the executive IP is flowing through policy 3, while traffic from the other computer uses policy 2.

Since policy 3 does not have any security profiles enabled, traffic from the executives is not being scanned for security events.

Seq.#	From	To	Source	Web Filter	Application Control	Action
1	lan	wan1	Executives			✓ Accept
2	lan	wan1	all	web default	APP default	✓ Accept
3	any	any	all			⊘ Deny

#	Policy ID	Date/Time	Source	Sent / Received
1	3	07:46:28	192.168.13.10	1.11 KB / 10.99 KB
2	3	07:46:28	192.168.13.10	1.10 KB / 9.13 KB
3	3	07:46:28	192.168.13.10	1.07 KB / 9.51 KB
4	3	07:46:28	192.168.13.10	1.16 KB / 12.48 KB
5	3	07:46:28	192.168.13.10	1.12 KB / 11.14 KB
6	2	07:45:48	192.168.13.144	8.41 KB / 10.79 KB
7	2	07:45:24	192.168.13.144	653 B / 4.99 KB
8	2	07:44:57	192.168.13.144	48 B / 0 B
9	2	07:44:47	192.168.13.144	2.51 KB / 1.28 KB
10	2	07:44:47	192.168.13.144	3.49 KB / 5.99 KB

# Wireless Networking

FortiOS WiFi networking provides a wide range of capabilities for integrating wireless networks into your organization's network architecture. Each WiFi network, or SSID, is represented by a virtual network interface to which you can apply firewall policies, security profiles, and other features in the same way you would for physical wired networks.

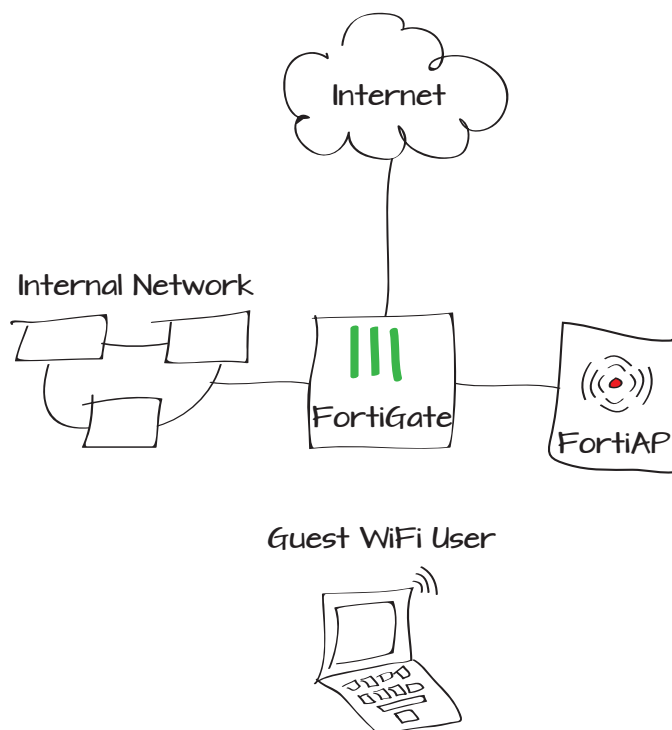
This chapter contains the following examples:

- [Setting up a temporary guest WiFi user](#)
- [Setting up a network using a FortiGate unit and a FortiAP unit](#)
- [Providing remote users access to the corporate network and Internet](#)
- [Assigning wireless users to different networks using dynamic VLANs](#)
- [Extending the range of a wireless network by using mesh topology](#)

# Setting up a temporary guest WiFi user

In this example, a temporary user account will be created and distributed to a guest user, allowing the guest to have wireless access to the Internet.

1. Connecting the FortiAP unit using the DMZ interface
2. Creating a WiFi guest user group
3. Creating an SSID using a captive portal
4. Creating a security policy to allow guest users Internet access
5. Creating a guest user management account
6. Results





# Connecting the FortiAP unit using the DMZ interface

Go to **System > Network > Interfaces**.  
Select the **dmz** interface.

Set the dmz interface to be **Dedicated to FortiAP**.

Connect the FortiAP to the DMZ interface.  
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and right-click on the FortiAP unit. Select **Authorize**.

Using the DMZ interface creates a secure network that will only grant access if it is explicitly allowed. This allows guest access to be carefully controlled.

Name

dmz (00:09:0F:99:39:6B)

Alias

Link Status

Up

Type

Physical Interface

Addressing mode

☐ Manual

☐ DHCP

☐ PPPoE

☒ Dedicate to FortiAP

IP/Network Mask

10.10.80.99/255.255.255.0

0 Connected FortiAPs/FortiSwitches

Administrative Access

☒ HTTPS

☒ PING

☐ HTTP

☒ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS

☐ PING

☐ HTTP

☐ FMG-Access

☐ SSH

☐ SNMP

☐ TELNET

Device Management

Detect and Identify Devices

☐

Comments

Write a comment...

0/255

Administrative Status

☒ Up

☐ Down

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients
-	FAP2283U11022065		10.10.80.100	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0	Radio 1: 0 Radio 2: 0

Edit

Delete

Authorize

Restart

Upgrade

## Creating a WiFi guest user group

Go to **User & Device > User > User Groups**.

Create a new group, setting **Type** to **Guest**, **User ID** to **Email**, and **Password** to **Auto-Generate**.

These guest user accounts are temporary and will expire four hours after the first login.

## Creating an SSID using a captive portal

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID. Set **Traffic Mode** to **Tunnel to Wireless Controller** and enable **DHCP Server**, taking note of the IP range assigned.

Under **WiFi Settings**, set **Security Mode** to **Captive Portal** and **User Groups** to the new guest user group.

A Captive Portal will intercept connections to the wireless network and display a login screen on the guest user's device. The guest must then authenticate with the portal to gain access to the wireless network.

Name

Type ☐ Firewall ☐ Fortinet Single Sign-On (FSSO) ☒ Guest ☐ RADIUS Single Sign-On (RSSO)

User ID

Password

☐ Enable Name

☒ Enable Sponsor

☒ Enable Company

☒ Enable Email

☐ Enable Phone Number ☐ FortiGuard Messaging Service ☐ Custom - SMS Provider: No SMS providers configured

Expire Type

Default Expire Time

☐ Enable Batch Guest Account Creation

Name

Type

Traffic Mode

IP/Network Mask

Administrative Access ☒ HTTPS ☒ PING ☐ HTTP ☐ FMG-Access ☒ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

IPv6 Administrative Access ☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ SSH ☐ SNMP ☐ TELNET

DHCP Server ☒ Enable

Address Range

Starting IP	End IP
10.10.10.2	10.10.10.254

Netmask

Default Gateway ☒ Same as Interface IP ☐ Specify

DNS Server ☒ Same as System DNS ☐ Specify

[Advanced...](#)

WiFi Settings

SSID

Security Mode

Customize Portal Messages ☐

User Groups

Maximum Clients ☐

# Creating a security policy to allow guest users Internet access

Go to **Firewall Objects > Address > Addresses.**

Create a firewall address for the guest WiFi users. Use the DHCP IP range for **Subnet/IP Range** and set the **Interface** to the wireless interface.

Go to **Policy > Policy > Policy.**

Create a security policy allowing guest users to have wireless access to the Internet.

Set **Incoming Interface** to the wireless interface, **Outgoing Interface** to your Internet-facing interface, and **Source Address** to the guest WiFi users group.


Policy Type

☒ Firewall ☐ VPN



Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity


Incoming Interface

WLAN (SSID: Guest WiFi Access) 



Source Address

 Guest WiFi Users 



Outgoing Interface

internal 



Destination Address

 Internal Wired Network 



Schedule

 always 

Service

 ALL 

Action

 ACCEPT 

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Click to add...

## Creating a guest user management account

Optionally, you can create an administrator that is used only to create guest accounts. Access to this account can be given to a receptionist, to simplify the process of making new accounts.

Go to **System > Admin > Administrators**.

Create a new account. Set the **Type** to **Regular** and set a **Password**. Enable **Restrict to Provision Guest Accounts** and set **Guest Groups** to the WiFi guest user group.

Administrator	<input type="text" value="Receptionist"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Comments	<input type="text" value="For providing wifi access to guests"/> 35/255

---

Contact Info

☐ Email Address

☐ SMS ☒ FortiGuard Messaging Service ☐ Custom

Phone Number

---


☐ Enable Two-factor Authentication

---

☐ Restrict this Admin Login from Trusted Hosts Only

---

☒ Restrict to Provision Guest Accounts

Guest Groups  

# Results

Log in to the FortiGate unit using the guest user management account. Go to **User & Device > User > Guest Management** and select **Create New**.

Use a guest's email account to create a new user ID.

The FortiGate unit generates a user account and password. This account is only valid for four hours (the default time limit for the guest user group).

The guest can now log in using the FortiGate Captive Portal. Once authenticated, the guest is able to connect wirelessly to the Internet.

User ID	Use Email Address
Password	Auto Generated
Sponsor	<input type="text" value="Terry White"/> Optional
Company	<input type="text" value="BigCo"/> Optional
Email	<input type="text" value="pbrown@bigco.com"/>
Expiration	<input type="text" value="2013-04-16 12:51"/>

## User Successfully Created

User ID	pbrown@bigco.com
Password	X876Yq
Company	BigCo
Sponsor	Terry White
Email	pbrown@bigco.com
Expiration	2013-04-16 12:51:00
Send	 

**FORTINET**

**Terms and Disclaimer Agreement**

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering,

☒ I accept the terms and disclaimer agreement

Authentication for SSID: Guest WiFi Access

Please enter your username and password to continue

Username:

Password:

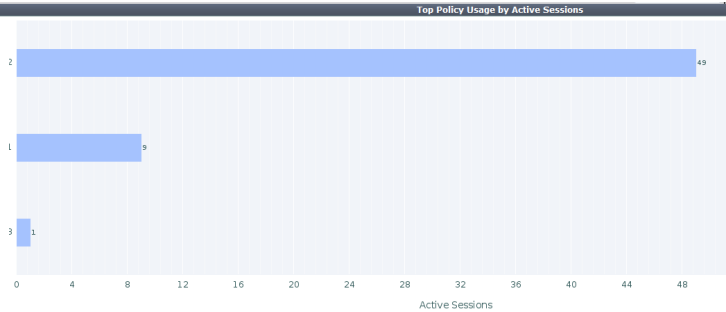
Continue

To verify that the guest user logged in successfully, go to **WiFi Controller > Monitor > Client Monitor**.

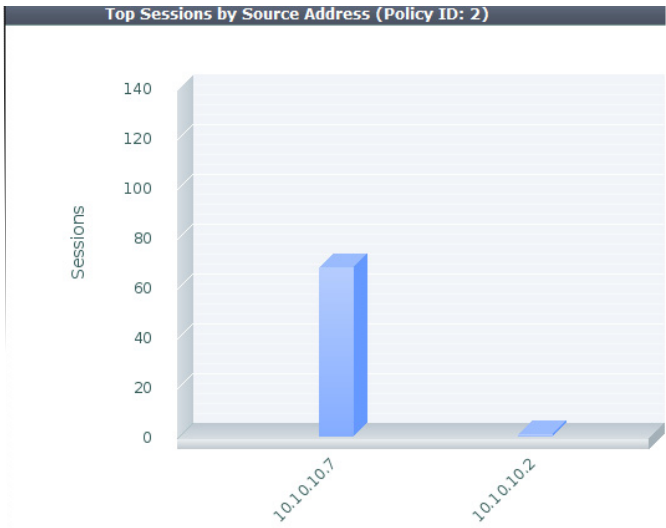
Go to **Policy > Monitor > Policy Monitor** and verify the active sessions.

Select one of the bars to view more information about a session.

SSID	FortiAP	User	IP	
Guest WiFi Access	FAP22B3U11022065 (2)	 pbrown@bigco.com	10.10.10.7	 70:f1



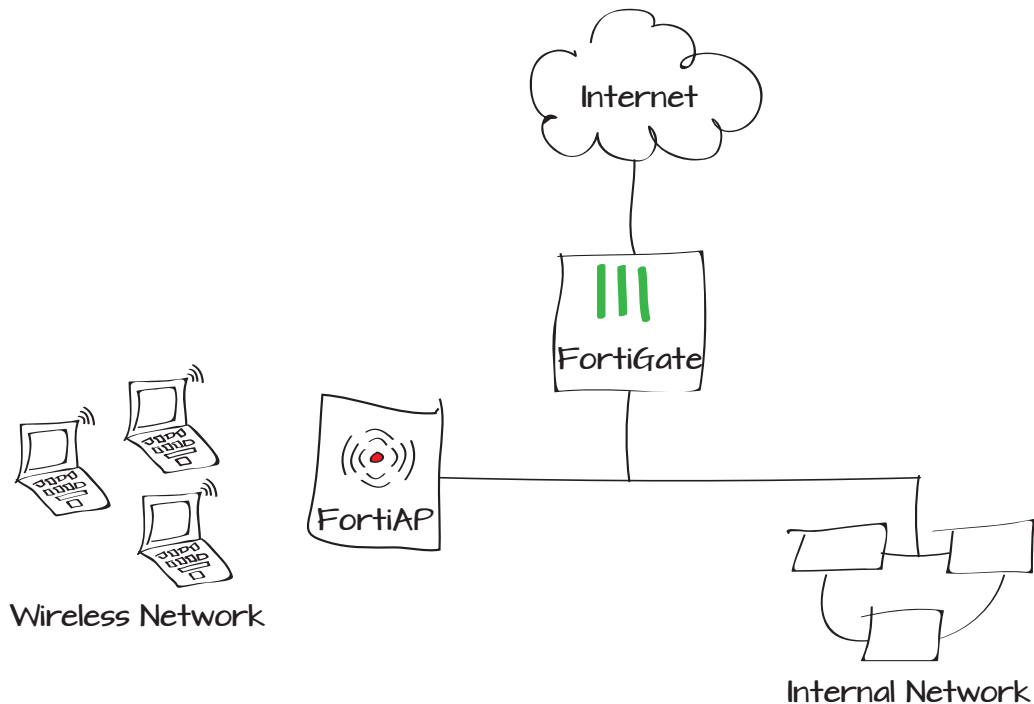
Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
2	WLAN	wan1	✓	49	31.88 MB	50,434
1	internal	wan1	✓	9	2.97 MB	13,133
3	WLAN	internal	✓	1	219.71 KB	358



# Setting up a network using a FortiGate unit and a FortiAP unit

This example sets up a wired network and a wireless network that are in the same subnet. This will allow wireless and wired users to share network resources.

1. Configuring the internal wired network to use DHCP
2. Creating the internal wireless network
3. Results



# Configuring the internal wired network to use DHCP

Edit the internal interface.

Set **Addressing mode** to **Manual** and enable **DHCP server**. Take note of the IP range.

Go to **Firewall Objects > Address > Addresses**.

Set **Type** to **IP Range** and set **Subnet/IP Range** to use the IP range from the DHCP server.

Name

internal (00:09:0F:7E:88:26)

Alias

Link Status

Up

Type

Physical Interface

Addressing mode

☒ Manual ☐ DHCP ☐ PPPoE ☐ Dedicate to FortiAP

IP/Network Mask

192.168.1.99/255.255.255.0

IPv6 Address

::/0

Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP

☐ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access ☐ Auto IPsec Request

IPv6 Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access ☐ CAPWAP

☐ SSH ☐ SNMP ☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New

Edit

Delete

Starting IP	End IP
192.168.1.100	192.168.1.254

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP ☐ Specify

DNS Server

☒ Same as System DNS ☐ Specify

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal network

Color

[Change]

Type

IP Range

Subnet / IP Range

192.168.1.110-192.168.1.210

Interface

wan2

Show in Address List

☒

Comments

Write a comment...

0/255



Go to **Policy > Policy > Policy**.

Create a security policy allowing users on the wired network to access the Internet.

## Creating the internal wireless network

Connect the FortiAP to the internal interface. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and right-click on the FortiAP unit. Select **Authorize**.



It may take a few minutes for the FortiAP unit to appear on the **Managed FortiAPs** list.

Policy Type: ☒ Firewall ☐ SSL-VPN

Policy Subtype: ☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface: internal

Source Address: Internal network

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

☐ Use Central NAT Table

Click to add...

**Logging Options**

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Mesh	Access Point	State	Connected Via	SSIDs	Chann
-	FAP22B3U11022065	?	192.168.1.110	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0

Edit

Delete

Authorize

Restart

Upgrade

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Ensure the **Traffic Mode** is set to **Local** bridge with FortiAP's Interface.



Bridge mode is more efficient than Tunnel mode, as it uses the CAPWAP tunnel for authentication only. Bridge mode is also required in order to have a wired and wireless network be on the same subnet.

Go to **WiFi Controller > WiFi Network > Custom AP Profiles**. Select **Create New**.

Set **SSID** for both **Radio 1** and **Radio 2** to the new SSID.

NameWLAN

TypeWiFi SSID

Traffic ModeLocal bridge with FortiAP's Inter...

WiFi Settings

SSIDMy\_SSID

Security ModeWPA/WPA2-Personal

Data EncryptionAES TKIP TKIP-AES

Pre-shared Key..... (8 - 63 characters)

Maximum Clients

Comments

Write a comment...0/255

Radio 1

ModeDisable Access Point Dedicated Monitor

Background ScanDisable Enable

WIDS Profile

Radio Resource Provision

Client Load BalancingFrequency Handoff AP Handoff

Band802.11an\_5G

20/40 MHz Channel Width

Channel36 40 44 48 149 153 157 161 165

Auto TX Power ControlDisable Enable

TX Power

SSID

Availablefortinet.mesh.root (Mest

SelectedMy\_SSID

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. Edit the FortiAP unit.

Under **Wireless Settings**, set **AP Profile** to use the new profile.

## Results

Users connected to the new SSID will be able to access the Internet. The wireless devices will be in the same subnet as the internal wired network.

Go to **WiFi Controller > Monitor > Client Monitor** to see WiFi users and their IP addresses.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that the same policy controls both wired and wireless traffic.

Serial Number	FAP22B3U11022065
Name	
Description	<a href="#">[Change]</a>
<b>Managed AP Status</b>	
Status	Online
Connected Via	Ethernet (192.168.1.110)
Base MAC Address	00:09:0f:35:6d:40
Join Time	03/22/13 10:38
Clients	0
FortiAP OS Version	FAP22B-v5.0-build031 <a href="#">[Upgrade]</a>
State	Authorized <a href="#">Deauthorize</a> <a href="#">Restart</a>
<b>Wireless Settings</b>	
AP Profile	MyProfile <a href="#">[Apply]</a>
<b>Radio 1</b>	
Mode	Access Point
Band	802.11an_5G
Channel	36, 40, 44, 48, 149, 153, 157, 161, 165
<b>Radio 2</b>	
Mode	Access Point
Band	802.11bgn_2.4G
Channel	1, 6, 11

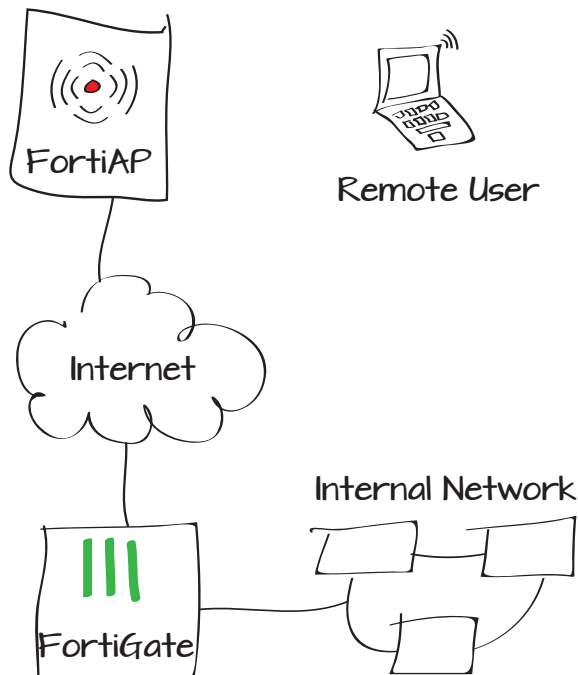
SSID	FortiAP	IP	Device	Auth	Channel	Bandwidth Tx/Rx
My_SSID	FAP22B3U11022065 (1)	192.168.1.111	84:29:99:be:54:dc	Pass	36	560 bps

Src Interface	Dst Interface	Src	Dst	Policy ID	Service	Sen
lan	wan1	192.168.1.111	74.121.50.17	1	HTTP	1.02 KB
lan	wan1	192.168.1.111	184.28.198.224	1	HTTP	940 B /
lan	wan1	192.168.1.112	208.91.112.132	1	HTTP	964 B /
lan	wan1	192.168.1.112	208.91.112.132	1	HTTP	924 B /
lan	wan1	192.168.1.112	8.8.8.8	1	DNS	62 B / 1
lan	wan1	192.168.1.112	208.91.112.133	1	HTTP	3.14 KB
lan	wan1	192.168.1.112	208.91.112.133	1	HTTP	924 B /
lan	wan1	192.168.1.112	173.194.64.147	1	HTTPS	1.59 KB
lan	wan1	192.168.1.111	192.168.110.9	1	DNS	71 B / 5
lan	wan1	192.168.1.111	17.164.0.8	1	HTTPS	2.68 KB

# Providing remote users access to the corporate network and Internet

In this example, a user in a remote location, such as a hotel or their home, will use a FortiAP unit to securely connect to the corporate network and browse the Internet from behind the corporate firewall.

1. Preauthorizing the FortiAP unit on the FortiGate unit
2. Creating an SSID and firewall addresses
3. Creating security policies
4. Configuring the FortiAP unit to connect to the FortiGate unit
5. Connecting to the FortiGate unit remotely
6. Results



# Pre-authorizing the FortiAP unit on the FortiGate unit

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Add a new FortiAP unit and enter the unit's **Serial Number** (in the example, *FAP11C3X13000412*).

The FortiAP unit will appear on the list of Managed FortiAPs as authorized and offline.'

# Creating an SSID and a firewall addresses

Go to **WiFi Controller > WiFi Network > SSID**. Select **Create New**.

Enable the **DHCP Server** and make note of the IP range.

Configure the **WiFi Settings** with a unique **SSID** name and **Pre-shared Key**.

Serial Number

FAP11C3X13000412

Name

Comments

Write a comment...0/35

State

Authorized

Wireless Settings

☒ Enable WiFi Radio

SSID

☒ Automatically Inherit all SSIDs

☐ Select SSIDs

Auto TX Power Control

☒ Disable

☐ Enable

TX Power

100 %

Access Point	State	Connected Via	SSIDs	Channel
FAP11C3X13000412		-	Radio 1: All	Radio 1: 0

Name

WLAN\_1

Type

WiFi SSID

Traffic Mode

Tunnel to Wireless Controller

IP/Network Mask

10.80.10.99/255.255.255.0

Administrative Access

☐ HTTPS☐ PING☐ HTTP☐ FMG-Access

☐ SSH☐ SNMP☐ TELNET☐ FCT-Access☐ Auto IPsec Request

DHCP Server

☒ Enable

Create NewEditDelete

Starting IP	End IP
10.80.10.100	10.80.10.254

Netmask

255.255.255.0

Default Gateway

☒ Same as Interface IP

☐ Specify

DNS Server

☒ Same as System DNS

☐ Specify

Advanced...

WiFi Settings

SSID

RemoteWiFi

Security Mode

WPA/WPA2-Personal

Data Encryption

☒ AES

☐ TKIP

☐ TKIP-AES

Pre-shared Key

.....

(8 - 63 characters)

Go to **Firewall Objects > Address > Addresses**. Create addresses for both the remote users and the corporate network.

For the remote users, set **Type** to **IP Range**. The range for the remote users should be within the range used for the DHCP server. Set **Interface** to the new SSID.

For the corporate network, set **Type** to **Subnet** and use the corporate network’s IP address. Set **Interface** to an internal interface.

## Creating security policies

Go to **Policy > Policy > Policy**.

Create a policy that allows remote wireless users to access the Internet. Set the **Incoming Interface** to the SSID and the **Outgoing Interface** as your Internet-facing interface.

Category

☒ Address ☐ IPv6 Address

Name

Wireless\_Users

Type

IP Range

Subnet / IP Range

10.80.10.100-10.80.10.200

Interface

WLAN\_1 (SSID: RemoteWiFi)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address

Name

Corp\_Network

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

internal

Show in Address List

☒

Comments

Write a comment... 0

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

WLAN\_1 (SSID: RemoteWiFi) +

Source Address

Wireless\_Users +

Outgoing Interface

wan1 +

Destination Address

all +

Schedule

always

Service

ALL +

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

Create a second policy for remote wireless users to access the corporate network. Again, set the **Incoming Interface** to the SSID but now the **Outgoing Interface** is an internal interface.

## Configuring the FortiAP unit to connect to the corporate FortiGate unit

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and note the IP Address assigned to your FortiAP.

Enter the address into your browser's address bar to access your FortiAP web manager.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☒ Enable NAT

☒ Use Destination Interface Address

☐ Use Dynamic IP Pool

Logging Options

☐ No Log

☐ Log Security Events

☒ Log all Sessions

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

WLAN\_1 (SSID: RemoteWiFi)

Wireless\_Users

internal

Corp\_Network

always

ALL

ACCEPT

☐ Fixed Port

Click to add...

Access Point	State	Connected Via	SSIDs
FAP11C3X13000412		10.10.10.2	Radio 1: All

In the **System Information** tab, enter the **AC IP Address** of the public facing interface of the corporate FortiGate unit. The Internet-facing interface is also the public facing interface. To locate this IP address, go to **System > Network > Interfaces**.

The FortiAP will search for this FortiGate interface when it tries to connect.

The remote user may now take this device to the desired remote location to connect securely to the corporate FortiGate unit.

## Connecting to the corporate FortiGate remotely

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power.

Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller.

The remote user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

AC Discovery Type	<input checked="" type="radio"/> Auto <input type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> DNS <input type="radio"/> Broadcast <input type="radio"/> Multicast
AC Control Port	<input type="text" value="5246"/>
AC IP Address 1	<input type="text" value="172.20.120.141"/>
AC IP Address 2	<input type="text"/>
AC IP Address 3	<input type="text"/>
AC Host Name 1	<input type="text" value="_capwap-control._udp."/>
AC Host Name 2	<input type="text"/>
AC Host Name 3	<input type="text"/>
AC Discovery Multicast Address	<input type="text" value="224.0.1.140"/>
AC Discovery DHCP Option Code	<input type="text" value="138"/>
AC Data Channel Security	<input type="radio"/> Clear Text <input type="radio"/> DTLS Enabled <input checked="" type="radio"/> Clear Text or DTLS Enabled



# Results

Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs.

Select an entry to view more information about remote traffic to the corporate network and to the Internet.

Refresh		Column Settings					
Device	Auth	IP	FortiAP	SSID	Channel	Bandwidth Tx/Rx	Sig
84:29:99:be:54:dc	Pass	10.80.10.100	FortiAP 220B (1)	RemoteWiFi	44	0 Kbps	
70:f1:a1:54:f6:27	Pass	10.80.10.103	FortiAP 220B (2)	RemoteWiFi	6	47 Kbps	

#	Date/Time	Device	Src	Dst	Src Interface	Dst Interface	Policy ID	Sig
1	3 seconds ago		10.80.10.103	213.199.179.151	WLAN_1	wan1	10	172
2	4 seconds ago		10.80.10.103	157.55.130.147	WLAN_1	wan1	10	176
3	3 seconds ago		10.80.10.103	172.20.120.235	WLAN_1	wan1	10	140
4	4 seconds ago		10.80.10.103	207.112.47.253	WLAN_1	wan1	10	435
5	6 seconds ago		10.80.10.103	172.20.181.253	WLAN_1	wan1	10	0 B
6	8 seconds ago		10.80.10.103	192.168.1.112	WLAN_1	internal	6	0 B
7	8 seconds ago		10.80.10.101	173.194.76.109	WLAN_1	wan1	10	12.

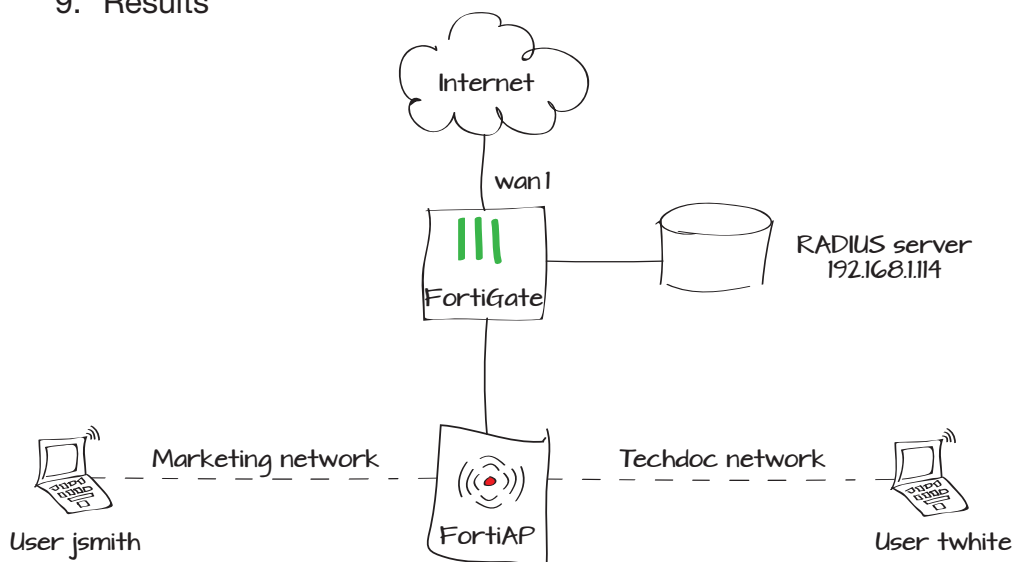
Dst	192.168.1.112	Virtual Domain	root
Received	0	Source Country	Reserved
Src NAT IP	192.168.1.99	Sent / Received	0 B / 0 B
Duration	0	Sent	0
Src NAT Port	55873	Application Details	
Service	RDP	Protocol	6
Destination Country	Reserved	Dst Port	3389
roll	65528	Status	start
Timestamp	Wed Nov 7 10:20:54 2012	Sequence Number	195221
Policy ID	6	Src Interface	WLAN_1
Src	10.80.10.103	Level	notice
Src Port	55873	logid	15
Sub Type	forward	Threat	
Tran Display	snat	Date/Time	8 seconds ago (Wed Nov 7 10:20:54 2012)
Dst Interface	internal		

Dst	157.55.130.147	Virtual Domain	root
Received	102	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	176 B / 102 B
Duration	181	Sent	176
Src NAT Port	37023	Application Details	
Service	40046/udp	Protocol	17
Destination Country	United States	Dst Port	40046
roll	65528	Status	accept
Timestamp	Wed Nov 7 10:20:58 2012	Tran Display	snat
Sequence Number	194834	Policy ID	10
Src Interface	WLAN_1	Src	10.80.10.103
Sent Packets	1	Level	notice
Src Port	37023	logid	13
Sub Type	forward	Threat	
Received Packets	1	Date/Time	4 seconds ago (Wed Nov 7 10:20:58 2012)
Dst Interface	wan1		

# Assigning wireless users to different networks using dynamic VLANs

Dynamic virtual LANs (VLANs) are used to assign wireless users to different networks without requiring the use of multiple SSIDs. This example creates dynamic VLANs for the Techdoc and Marketing departments, with a RADIUS server used for authentication.

1. Connecting the FortiAP unit
2. Creating an SSID with dynamic VLANs enabled
3. Creating and assigning a custom AP profile
4. Creating the VLAN interfaces
5. Creating security policies for both networks
6. Configuring a connection to the RADIUS server
7. Creating the RADIUS client
8. Creating network policies on the RADIUS client
9. Results



# Connecting the FortiAP unit

Connect the FortiAP to the internal interface. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and right-click on the FortiAP unit. Select **Authorize**.



It may take a few minutes for the FortiAP unit to appear on the Managed FortiAP list.

# Creating an SSID with dynamic VLANs enabled

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID. Set **Traffic Mode** to **Local bridge with FortiAP's Interface**.



Dynamic VLANs can also be used with a FortiAP in Tunnel Mode. The only difference in the configuration occurs when creating VLAN interfaces, as the initial creation must occur using the CLI.

Mesh	Access Point	State	Connected Via	
-	FAP22B3U11024253	?	192.168.1.112	

Authorize

Deauthorize

Restart

Refresh

Upgrade

Assign Profile

Name

Dynamic\_VLAN

Type

WiFi SSID

Traffic Mode

Local bridge with FortiAP's Interf...

WiFi Settings

SSID

Dynamic\_VLAN\_SSID

Security Mode

WPA/WPA2-Enterprise

Data Encryption

AES

TKIP

TKIP-AES

Authentication

RADIUS Server

Usergroup

My\_Radius\_Server

Maximum Clients

Comments

Write a comment...

0/255

Administrative Status

Up

Down

Go to **System > Dashboard > Status**.  
Enable dynamic VLANs on the FortiAP and set the default VLAN ID (10 in the example) by entering the following in the CLI Console:

## Creating and assigning a custom AP profile

Go to **WiFi Controller > WiFi Network > Custom AP profiles**.

Create a new profile and select the new SSID for both Radio 1 and Radio 2.

```
config wireless-controller vap
  edit Dynamic_VLAN
    set vlanid 10
    set dynamic-vlan enable
  end
end
```

Name

My\_Profile

Comments

Write a comment...

0/255

Platform

FAP220B/FAP221B

▼ Radio 1

Mode

☐ Disable

☒ Access Point

☐ Dedicated Monitor

Background Scan

☒ Disable

☐ Enable

WIDS Profile

Radio Resource Provision

☐

Client Load Balancing

☐ Frequency Handoff

☐ AP Handoff

Band

802.11an\_5G

20/40 MHz Channel Width

☐

Channel

☒ 36

☒ 40

☒ 44

☒ 48

☒ 149

☒ 153

☒ 157

☒ 161

☒ 165

Auto TX Power Control

☒ Disable

☐ Enable

TX Power

100 %

SSID

Available

Selected

▶ Radio 2

▼ Access Point

FAP22B3U11024253

▼ State

▼ Connected Via

10.10.80.100

▼ SSIDs

Radio 1: FortiDocs1  
Radio 2: FortiDocs1

Edit

Delete

Authorize

Deauthorize

Restart

Refresh

Upgrade

Assign Profile

FAP220B

FAP220B-default

My\_Profile

Automatic Profile

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Right-click on the FortiAP unit. Select **Assign Profile** and set it to the new AP profile.

# Creating the VLAN interfaces

Go to **System > Network > Interface**.

Create the VLAN interface for marketing-100.  
Enable **DHCP Server**.

Create the VLAN interface for techdoc-200.  
Enable **DHCP Server**.

Namemarketing-100

TypeVLAN

InterfaceDynamic\_VLAN\_SSID

VLAN ID100

Addressing modeManualDHCPPPPoE

IP/Network Mask172.16.10.1/255.255.255.0

IPv6 Address::/0

Administrative Access

HTTPSPINGHTTPFMG-AccessCAPWAP

SSHSNMPTELNETFCT-Access

IPv6 Administrative Access

HTTPSPINGHTTPFMG-AccessCAPWAP

SSHSNMPTELNET

DHCP Server

Enable

Address Range

Create NewEditDelete

Starting IP	End IP
172.16.10.2	172.16.10.254

Netmask255.255.255.0

Nametechdoc-200

TypeVLAN

InterfaceDynamic\_VLAN\_SSID

VLAN ID200

Addressing modeManualDHCPPPPoE

IP/Network Mask172.16.20.1/255.255.255.0

IPv6 Address::/0

Administrative Access

HTTPSPINGHTTPFMG-AccessCAPWAP

SSHSNMPTELNETFCT-Access

IPv6 Administrative Access

HTTPSPINGHTTPFMG-AccessCAPWAP

SSHSNMPTELNET

DHCP Server

Enable

Address Range

Create NewEditDelete

Starting IP	End IP
172.16.20.2	172.16.20.254








Netmask255.255.255.0








## Creating security policies for both networks

Go to **Policy > Policy > Policy**.

Create a policy that allows outbound traffic from marketing-100. Set **Incoming Interface** to marketing-100 and **Outgoing Interface** to the Internet-facing interface.

Create another new policy that allows outbound traffic from techdoc-200. Set **Incoming Interface** to techdoc-200 and **Outgoing Interface** to the Internet-facing interface.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> SSL-VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	marketing-100 
Source Address	all 
Outgoing Interface	wan1 
Destination Address	all 
Schedule	always 
Service	ALL 
Action	ACCEPT 
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> SSL-VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	techdoc-200 
Source Address	all 
Outgoing Interface	wan1 
Destination Address	all 
Schedule	always 
Service	ALL 
Action	ACCEPT 
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	

## Configuring a connection to the RADIUS server



This example uses NPS on Windows Server 2008. The RADIUS server has already been configured with the user group Techdoc, with member twhite, and the user group Marketing, with member jsmith.

Go to **User & Device > Authentication > RADIUS Servers**. Select **Create New**.

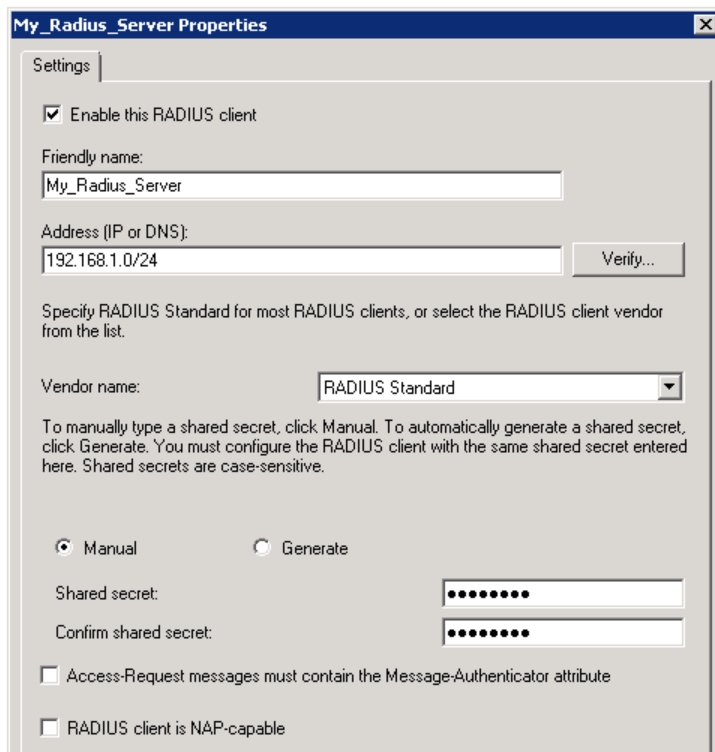
Configure the connection to your RADIUS server, setting both the **Primary Sever Name/IP** and the **Primary Server Secret**. Select **Use Default Authentication Scheme**.

Name	<input type="text" value="My_Radius_Server"/>	
Primary Server Name/IP	<input type="text" value="192.168.1.114"/>	
Primary Server Secret	<input type="password" value="....."/>	<input type="button" value="Test"/>
Secondary Server Name/IP	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test"/>
Authentication Scheme	<input checked="" type="radio"/> Use Default Authentication Scheme <input type="radio"/> Specify Authentication Protocol <div><input type="text" value="PAP"/> ▼</div>	
NAS IP/Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/> Enable	

## Creating the RADIUS client

Connect to the RADIUS server.

Open the **Server Manager** and create a new RADIUS client.



The screenshot shows the 'My\_Radius\_Server Properties' dialog box with the 'Settings' tab selected. The 'Enable this RADIUS client' checkbox is checked. The 'Friendly name' field contains 'My\_Radius\_Server'. The 'Address (IP or DNS)' field contains '192.168.1.0/24', with a 'Verify...' button to its right. Below this, a text label reads: 'Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.' The 'Vendor name' dropdown menu is set to 'RADIUS Standard'. A paragraph of instructions follows: 'To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.' There are two radio buttons: 'Manual' (selected) and 'Generate'. Below these are two text fields for 'Shared secret' and 'Confirm shared secret', both masked with dots. At the bottom, there are two unchecked checkboxes: 'Access-Request messages must contain the Message-Authenticator attribute' and 'RADIUS client is NAP-capable'.

My\_Radius\_Server Properties

Settings

☒ Enable this RADIUS client

Friendly name:  
My\_Radius\_Server

Address (IP or DNS):  
192.168.1.0/24 Verify...

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☒ Manual ☐ Generate

Shared secret: .....

Confirm shared secret: .....

☐ Access-Request messages must contain the Message-Authenticator attribute

☐ RADIUS client is NAP-capable



# Creating network policies on the RADIUS client

Create a network policy for the TechDoc department that uses the techdoc-200 VLAN.

Techdoc Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.

☐ Deny access. Deny access if the connection request matches this policy.

☐ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:

☐ Vendor specific:

OK

Cancel

Apply

Techdoc Properties

Overview | Conditions | Constraints | Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
User Groups	FORTIDOCSTechdoc

Condition description:

The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Add...

Edit...

Remove

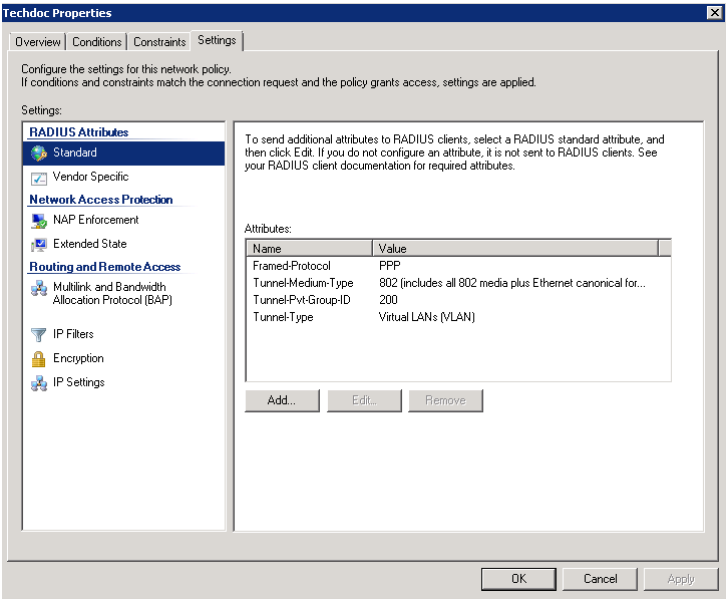
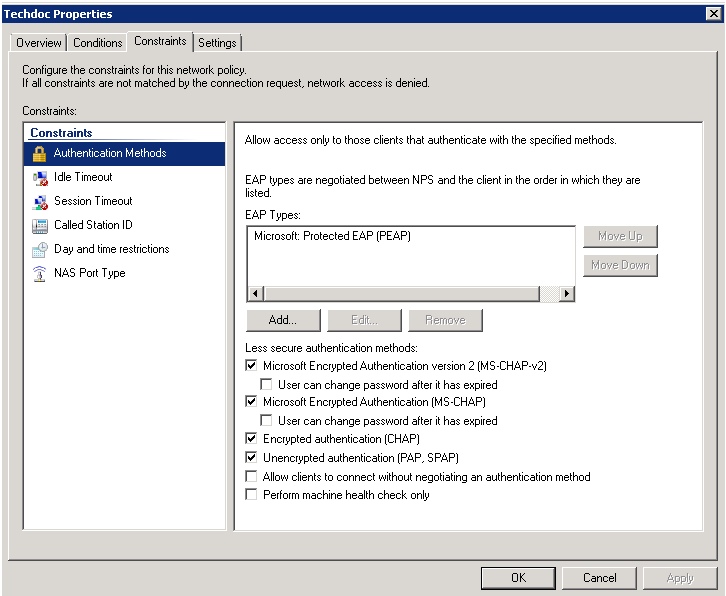
OK

Cancel

Apply

Set **Tunnel-Pvt-Group** to 200, the VLAN ID of techdoc-200, and **Tunnel-Type** to Virtual LANs (VLAN)

Repeat this procedure to create a network policy for the Marketing depart that uses the marketing-100 VLAN.



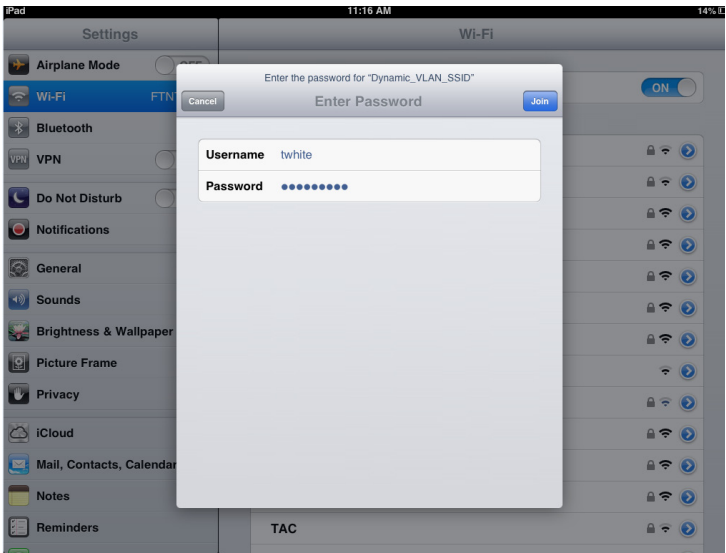
# Results

The SSID will appear in a list of available wireless networks on the users' devices. Both twhite and jsmith can connect to the SSID with their credentials.

If a certificate warning message appears, accept the certificate.

Go to **WiFi Controller > Monitor > Client Monitor**. Both users are shown using the same SSID.

Go to **Log & Report > Traffic Log > Forward Traffic Log**. Traffic flows through both policies, using the provided credentials.



SSID	FortiAP	User	IP
Dynamic_VLAN	FAP22B3U11024253 (2)	jsmith	172.16.10.3
Dynamic_VLAN	FAP22B3U11024253 (1)	twhite	172.16.20.2

Date/Time	Src Interface	Dst Interface	Src	Policy ID
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:08:12	techdoc-200	wan1	172.16.20.2	18
11:07:10	marketing-100	wan1	172.16.10.3	15
11:07:10	marketing-100	wan1	172.16.10.3	15
11:07:10	marketing-100	wan1	172.16.10.3	15
11:07:10	marketing-100	wan1	172.16.10.3	15
11:07:10	marketing-100	wan1	172.16.10.3	15

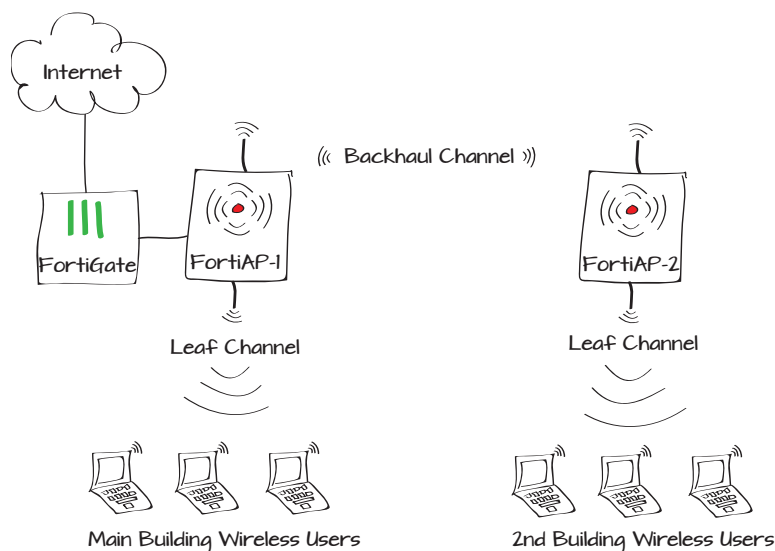
# Extending the range of a wireless network by using mesh topology

This example demonstrates how to configure a FortiGate and two FortiAP wireless access point units to extend the reach and availability of a wireless network. This example simulates a company that has expanded into a second, nearby building that requires wireless access.



The FortiAP units used to create a wireless mesh must be models that have two radios.

1. Configuring an interface on the FortiGate for the APs
2. Creating two SSIDs
3. Creating a custom AP profile
4. Creating firewall addresses and an address group
5. Setting up and configuring the FortiAPs
6. Creating security policies on the FortiGate
7. Results



# Before you begin

The following models were used in this example: FortiGate-100D, FortiAP-220B, and FortiAP-221B.

The FortiGate unit is in Interface Mode (each physical port can be the interface to a distinct subnet), so that a single port, in this case 11, will be used for the sole purpose of interface for the wireless network.

The computers managing the network and FortiAPs are located on the internal network.

# Configuring an interface on the FortiGate for the APs

A dedicated network interface needs to be configured on the Fortigate that will be used only by the FortiAP units.

Go to **System > Network > Interfaces** and edit an available internal port (in the example, port11). Set **Addressing mode** to **Dedicate to FortiAP/FortiSwitch**.

Name

port11(00:09:0F:99:4B:F4)

Alias

FortiAP

Link Status

Up

Type

Physical Interface

Addressing mode

☐ Manual

☐ DHCP

☐ PPPoE

☒ Dedicate to FortiAP/FortiSwitch

IP/Network Mask

192.168.11.1/255.255.255.0

1 Connected FortiAPs/FortiSwitches

Device Management

Detect and Identify Devices

☐

Comments

Write a comment...

0/255

Administrative Status

☒ Up

☐ Down

# Creating two SSIDs

A wireless mesh requires two SSIDs: back-haul and leaf. The backhaul channel is the wireless connection between the two FortiAP units, while the leaf channel is used by individual clients to connect to the wireless network.

Go to **System > Network > Interfaces** and create the backhaul SSID.

Set **Type** to **WiFi SSID** and configure the **WiFi Settings** as needed.

Create the leaf SSID.

Set **Type** to **WiFi SSID**, enable **DHCP Server**, and configure the **WiFi Settings** as needed.

NameBackhaul.mesh

TypeWiFi SSID

Traffic ModeMesh Downlink

WiFi Settings

SSIDbackhaul-ssid

Security ModeWPA/WPA2-Personal

Data EncryptionAES TKIP TKIP-AES

Pre-shared Key\*\*\*\*\* (8 - 63 characters)

Nameleaf-ssid

TypeWiFi SSID

Traffic ModeTunnel to Wireless Controller

IP/Network Mask192.168.205.1/255.255.255.0

IPv6 Address::/0

Administrative Access

☒ HTTPS ☒ PING ☒ HTTP ☐ FMG-Access

☐ SSH ☐ SNMP ☐ TELNET ☐ FCT-Access

IPv6 Administrative Access

☐ HTTPS ☐ PING ☐ HTTP ☐ FMG-Access

☐ SSH ☐ SNMP ☐ TELNET

DHCP Server

☒ Enable

Address Range

Create New Edit Delete

Starting IP	End IP
192.168.205.5	192.168.205.254

Netmask255.255.255.0

Default GatewaySame as Interface IP Specify

DNS ServerSame as System DNS Specify

Advanced...

WiFi Settings

SSIDleaf-ssid

Security ModeWPA/WPA2-Personal

Data EncryptionAES TKIP TKIP-AES

Pre-shared Key\*\*\*\*\* (8 - 63 characters)

# Creating a custom AP profile

Go to **WiFi & Switch Controller > WiFi Network > Custom AP Profile**.

Create a new profile for the FortiAP model you are using.

Configure **Radio 1** for the backhaul channel and **Radio 2** for the leaf channel.

For the backhaul channel, set **Band** to **802.11an\_5G**. For the leaf channel, set **Band** to **802.11bgn\_2.4G**.



You may have to configure two custom AP profiles if your FortiAP units are different models that cannot use the same profile.

▼ Radio 1

Mode

☐ Disable ☒ Access Point ☐ Dedicated Monitor

Background Scan

☒ Disable ☐ Enable

WIDS Profile

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

802.11an\_5G

20/40 MHz Channel Width

☐

Channel

☒ 36 ☒ 40 ☒ 44 ☒ 48 ☒ 149 ☒ 153 ☒ 157 ☒ 161 ☒ 165

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

Available

Selected

leaf-ssid  
fortinet.mesh.root (Mesh S

backhaul-ssid (Mesh SSID

▼ Radio 2

Mode

☐ Disable ☒ Access Point ☐ Dedicated Monitor

Background Scan

☒ Disable ☐ Enable

WIDS Profile

Radio Resource Provision

☒

Client Load Balancing

☐ Frequency Handoff ☐ AP Handoff

Band

802.11bgn\_2.4G

Channel

☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Auto TX Power Control

☒ Disable ☐ Enable

TX Power

100 %

SSID

Available

Selected

backhaul-ssid (Mesh SSID  
fortinet.mesh.root (Mesh S

leaf-ssid

# Creating firewall addresses and an address group

Go to **Firewall Objects > Address > Addresses**.

Create a new address for the internal network.

Create an address for FortiAP-1.

Create an address for FortiAP-2.

Create an address for leaf channel users, using the DHCP range used by the leaf channel SSID.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal\_Network

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.150.0/255.255.255.0

Interface

LAN

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FortiAP1

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.11.2

Interface

port11 (FortiAP)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FortiAP2

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.11.3

Interface

port11 (FortiAP)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Leaf\_Wireless\_Subnet

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.205.0/255.255.255.0

Interface

leaf-ssid (SSID: leaf-ssid)

Show in Address List

☒

Comments

Write a comment... 0/255



Go to **Firewall > Address > Groups** and create a new group.

Add the FortiAP addresses to the group.

## Setting up and configuring the FortiAPs

In this example, the FortiAP-221B unit is FortiAP-1, while the FortiAP-220B is FortiAP-2.

### Preauthorize FortiAP-1

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**. Select **Create New**.

Enter the serial number of the FortiAP unit and give the Managed Access Point a name.

Group Name	<input type="text" value="Mesh_APs"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Color	[Change]
Show in Address List	<input checked="" type="checkbox"/>
Members	<div><div> FortiAP1</div><div> FortiAP2</div></div>

Serial Number	<input type="text" value="FP221"/>
Name	<input type="text" value="FortiAP-1"/>
Comments	<input type="text" value="Write a comment..."/> 0/35
State	Authorized
<b>Wireless Settings</b>	
<input checked="" type="checkbox"/> Enable WiFi Radio	
SSID	<div><input checked="" type="radio"/> Automatically Inherit all SSIDs</div> <div><input type="radio"/> Select SSIDs</div>
Auto TX Power Control	<div><input checked="" type="radio"/> Disable <input type="radio"/> Enable</div>
TX Power	<div> <input type="range" value="100"/> 100 %</div>

# Preauthorize FortiAP-2

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**. Select **Create New**.

Enter the serial number of the FortiAP and give the Managed Access Point a name.

The FortiAP list will now show both FortiAP units. Since they are not currently connected, they will appear greyed out.

# Apply the Custom AP profile

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**.

The same custom AP profile needs to be added to both the FortiAP units. Edit each one in turn.

Use the **[Change]** link to assign the custom AP profile.

Serial Number

FAP22B3

Name

FortiAP-2

Comments

Write a comment...0/35

State

Authorized

Wireless Settings

☒ Enable WiFi Radio

SSID

☒ Automatically Inherit all SSIDs

☐ Select SSIDs

Auto TX Power Control

☒ Disable

☐ Enable

TX Power

100 %

Mesh	Access Point	State	Connected Via	SSIDs	Channel
<input type="checkbox"/>	FortiAP-1	<input type="checkbox"/>	-	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0
<input type="checkbox"/>	FortiAP-2	<input type="checkbox"/>	-	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0

Serial Number

FP221B3X13019600

Name

FortiAP-1

Comments

Write a comment...0/35

Managed AP Status

Status

Online

Connected Via

Ethernet (192.168.11.2)

Base MAC Address

08:5b:0e:22:01:ae

Join Time

10/10/13 17:44

Clients

1

FortiAP OS Version

FP221B-v5.0-build048 [Upgrade]

State

Authorized 

Deauthorize

Restart

Wireless Settings

AP Profile

FAP22xB-Mesh [Change]

The FortiAP list now shows that the SSIDs have been added to the appropriate radios on the APs.

### Configure FortiAP-1 through its web interface

Certain parameters of the FortiAP units can only be configured by connecting to the unit directly, rather than through the FortiGate interface.

Reset the IP information of your computer to an address on the same subnet as the FortiAP. If the AP is in its factory default configuration, use the following address:

IP address: 192.168.1.100  
Subnet mask: 255.255.255.0  
Gateway: 192.168.1.1

Connect your computer to the FortiAP with an Ethernet cable. One end of the Ethernet cable connected to the network interface port of you computer and the other connected to the POE interface on the AP.

Access Point	State	Connected Via	SSIDs
FortiAP-1	✓	-	Radio 1: backhaul-ssid Radio 2: leaf-ssid
FortiAP-2	✓	-	Radio 1: backhaul-ssid Radio 2: leaf-ssid



Open a browser window and use the IP address of the FortiAP unit as the URL. The factory default IP address is 192.168.1.2. Login with the name: *admin*. Password is null, so just press Login.



If this does not work, use the reset button to return the FortiAP to default settings.

Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

Set **Uplink** to **Ethernet** and **AC Discovery Type** to **Auto**.

Once the changes have been made, you will not be able to connect to the FortiAP unit through the web interface, because it is no longer on the same subnet as your computer.

Do not reset the IP configuration on the computer yet as you still need to configure FortiAP #2 and the same addresses will be used on both sides of the Ethernet connection.

### Configure AP-2 through its web interface

As with the AP-1, connect to the web interface. Make sure to use the correct Ethernet port.

Network Configuration

Address Mode

☒ Static ☐ DHCP

Management VLAN ID

0

Local IP Address

192.168.11.2

Local Network Mask

255.255.255.0

Gateway IP

192.168.11.1

Administrative Access

☒ HTTP ☐ TELNET

Connectivity

Uplink

☒ Ethernet ☐ Mesh ☐ Ethernet with mesh backup support

WTP Configuration

AC Discovery Type

☒ Auto ☐ Static ☐ DHCP ☐ DNS ☐ Broadcast ☐ Multicast

AC Control Port

5246

AC IP Address 1

192.168.1.1



Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

Set **Uplink** is set to **Mesh**, the **AC Discover Type** to **Static**, and **AC IP Address 1** to the IP interface of the FortiGate port that is dedicated to the FortiAPs.

Reset the computer to its normal IP address configuration and login to the FortiGate unit.

Connect FortiAP-1 to the FortiGate interface dedicated to the FortiAPs (in the example, port 11).

Once the FortiAPs are configured and powered up, they should no longer be shown as online. The **Mesh** column will also show that FortiAP-2 is connected through a mesh to FortiAP-1.

Address Mode

☒ Static ☐ DHCP

Local IP Address

192.168.11.3

Local Network Mask

255.255.255.0

Gateway IP

192.168.11.1

Administrative Access

☒ HTTP ☐ TELNET

Uplink

☐ Ethernet ☒ Mesh ☐ Ethernet with mesh backup su

Mesh AP SSID

backhaul-ssid

Mesh AP Password

\*\*\*\*\*

Ethernet Bridge

☐

AC Discovery Type

☐ Auto ☒ Static ☐ DHCP ☐ DNS ☐ Broadcast

AC Control Port

5246

AC IP Address 1

192.168.1.1

AC IP Address 2

AC IP Address 3

AC Data Channel Security

☐ Clear Text ☐ DTLS Enabled ☒ Clear Text or DTLS

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients
⌵	FortiAP-1	✔	🌐 192.168.11.2	Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 1	Radio 1: 1 Radio 2: 0
⌵	FortiAP-2	✔	🌐 192.168.11.3	Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 6	Radio 1: 0 Radio 2: 1

## (Alternative) Configure AP-2 through its console port

FortiAP-2 in the example is a FAP-220B. This model includes a console port. This allows for the option of using the CLI to configure the unit.

Instead of an Ethernet cable, use a console cable to connect from your computer to the console port of FortiAP #2. The exact details of connecting will defer slightly based on whether the console cable is connected directly from a serial port or through a USB adapter and what operating system is on your computer, but once the connection has been made it proceeds as follows:

Using a utility like Putty or Terminal, connect to the CLI. For more details on connecting read the Quick Start Guide for the model.

Login with the credentials:

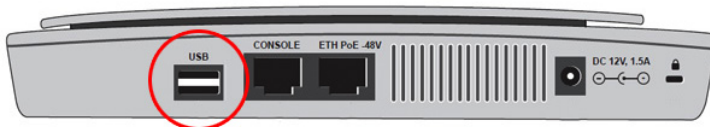
Username: admin

Password: <null>

Use the following commands to change the network configuration.

Change Address Mode to Static:

Set the IP address:



```
cfg -a ADDR_MODE=STATIC
cfg -c
```

```
cfg -a IPADDR=192.168.11.3
cfg -a AP_NETMASK:=255.255.255.0
cfg -a IPGW=192.168.11.1
cfg -c
```

Change Connectivity, remembering to choose a more secure password:

```
cfg -a MESH_AP_TYPE:=1
cfg -a MESH_AP_SSID:=backhaul-ssid
cfg -a MESH_AP_PASSWD:=12345678
cfg -c
```

Assign the discovery type to Static:

```
cfg -a AC_DISCOVERY_TYPE=1
cfg -c
```

Statically assign the IP address for the Access Controller (AC):

```
cfg -a AC_IPADDR=192.168.11.1
cfg -c
```

# Creating security policies on the FortiGate

Go to **Policy > Policy > Policy** and create a policy to allow wireless users out to Internet

Set **Incoming Interface** to the leaf SSID, **Source Address** to the address for leaf channel users, **Outgoing Interface** to your Internet-facing interface, and **Enable NAT**.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	leaf-ssid (SSID: leaf-ssid) +
Source Address	Leaf_Wireless_Subnet +
Outgoing Interface	wan1 +
Destination Address	all +
Schedule	always -
Service	ALL +
Action	ACCEPT -
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
Click to add...	

Create another policy to allow traffic to reach APs. This is primarily to allow access to the web interfaces of the FortiAPs, so if you wish you can limit the policy to only allow access to those IP addresses.

Set **Incoming Interface** to the internal network's interface (in the example, **LAN**), **Source Address** to the address for the internal network, **Outgoing Interface** to the port dedicated to the FortiAPs, and (optionally) **Destination Address** to the group containing both FortiAP addresses.



After policies are created, remember to place them at a proper point in the sequence so that they can be reached by the desired traffic but will not interfere with other traffic.

## Results

Wireless devices are now able to connect to the leaf SSID, even if they are only within the range of FortiAP-2.

There are several ways to verify that the wireless network has been extended over both FortiAP units.

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**.

You can see that **Radio 2** (leaf-ssid) on FortiAP-2 has one client connected to it, while the same SSID on FortiAP-1 does not.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☐ Enable NAT

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

LAN

Internal\_Network

port11 (FortiAP)

Mesh\_APs

always

HTTP

ACCEPT

SSIDs	Channel	Clients
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 1	Radio 1: 1 Radio 2: 0
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 6	Radio 1: 0 Radio 2: 1




Go to **WiFi & Switch Controller > Monitor > Client Monitor**.



The client monitor which SSID and FortiAP that a client is connected to. In the example, a client has successfully connected to the leaf SSID on FortiAP-2.

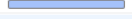
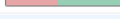
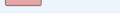
Go to **WiFi & Switch Controller > Monitor > Wireless Health**.

For information on the leaf channel, which uses the 2.4 GHz frequency, view the **Top Client Count Per-AP (2.4 GHz Band)** widget. In the example, the only SSID on that frequency is for the leaf channel, so the client using radio 1 on FortiAP-2 must be using that SSID.

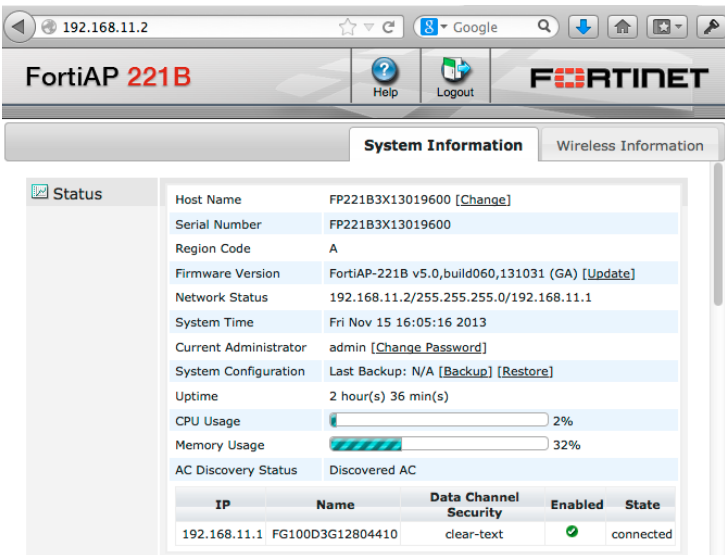
For information on the backhaul channel, which uses the 5 GHz frequency, view the **Top Client Count Per-AP (5 GHz Band)**. Again, in the example configuration, the only SSID on this frequency is for the backhaul channel.

SSID	FortiAP	User	IP	Device
leaf-ssid	FortiAP-2 (2)		192.168.205.5	 d8:30:62:9b:63:1b

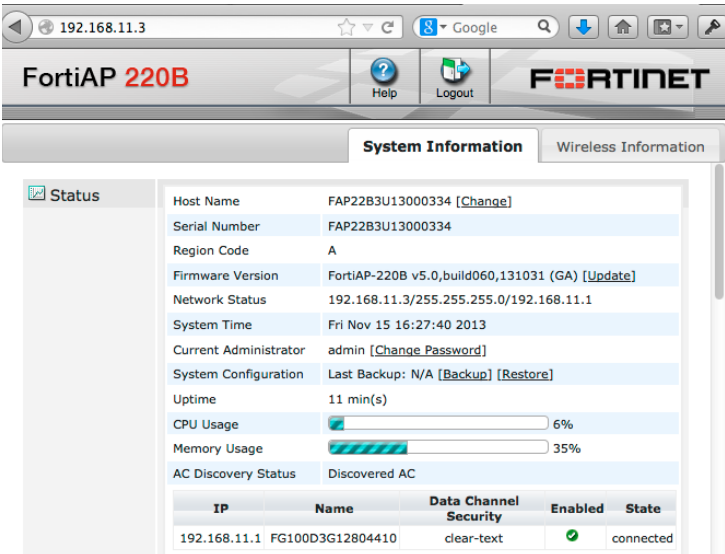
Top Client Count Per-AP (2.4 GHz Band)			
FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-2 (2)	1 	6	925 bps 
FortiAP-1 (2)	0	1	340 bps 

Top Client Count Per-AP (5 GHz Band)			
FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-1 (1)	1 	40	3.28 Kbps 
FortiAP-2 (1)	0	40	1018 bps 

Open a browser and verify that you can connect to the web interface of FortiAP-1, using the IP set in the configuration (in the example, *http://192.168.11.2*).



Connect to the web interface of FortiAP-2 using its assigned IP (in the example, *http://192.168.11.3*).



# IPv6

Internet Protocol version 6 (IPv6) is the most significant advance in traditional Internet communications protocol. The IPv6 address scheme is based on a 128-bit address, rather than the 32-bit addresses used by IPv4, allowing IPv6 to have a much higher address limit of over 340 undecillion possible addresses (that is 340 followed by 36 zeros). FortiGate units support IPv6 in a wide variety of network configurations.

This section contains the following examples:

- [Creating an IPv6 interface using SLAAC](#)

# Creating an IPv6 interface using SLAAC

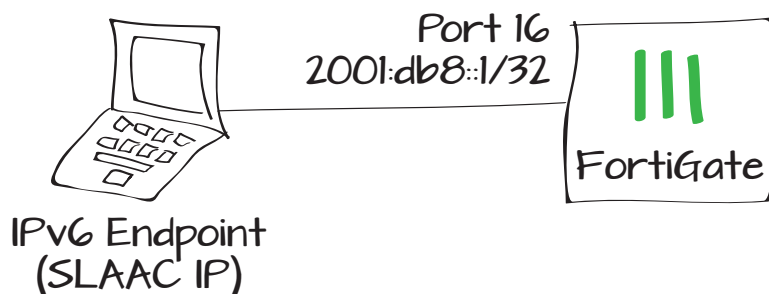
In this recipe you will learn how to configure an interface on your FortiGate to assign IPv6 addresses. Using Stateless Address Autoconfiguration (SLAAC), the IPv6 interface will automatically assign IPv6 addresses to any device that connects to that port.

This recipe assumes that your Internet connection is enabled for IPv6.



The IPv6 address block used in this recipe is reserved for documentation purposes and will not work in your environment. If you're not sure how to determine the correct IPv6 address for your environment, refer to the [FortiOS IPv6 Handbook Chapter](#).

1. Configuring the IPv6 network interface
2. Configuring the IPv6 firewall address
3. 'Bouncing' the IPv6 interface
4. Results



## Configuring the IPv6 network interface

Navigate to **System > Network > Interfaces** and choose (or create) an interface appropriate for your network.

In the example, we are using port16 as the IPv6 interface.

Set the **Addressing mode** to **Manual** and enter the **IP/Network Mask** and **IPv6 Address** for the interface.

Select the desired **Administrative Access** options.

Enabling router advertisements and configuring the IPv6 prefix list



This step must be performed in the CLI console.

In order for the IPv6 interface to autoconfigure IPv6 addresses, the interface must have router advertisements and specific IPv6 prefixes enabled.

Navigate to **System > Dashboard > Status** and scroll down to the **CLI Console**.

Enter the console and input the commands shown on the right.

Name	port16(00:09:0F:4E:0E:CE)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode <input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to FortiAP/FortiSwitch	
IP/Network Mask	<input type="text" value="10.10.116.1/255.255.255.0"/>
IPv6 Address	<input type="text" value="2001:db8::1/32"/>
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access
IPv6 Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> TELNET

```
config system interface
edit port16
config ipv6
set ip6-address 2001:db8::1/32
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8::/32
set autonomous-flag enable
set onlink-flag enable
next
end
end
end
```

## Configuring the IPv6 firewall address

Navigate to **Firewall Objects > Address > Addresses** and select **Create New > IPv6 Address**.

Under **Category**, ensure that **IPv6 Address** is selected.

Enter a **Name** for the firewall object and set the **IPv6 Address** to the address of the IPv6 interface.

## 'Bouncing' the IPv6 interface

You can now 'bounce' the IPv6 interface (bring the interface down and then back up). This causes a router advertisement using Neighbor Discovery Protocol, which performs address autoconfiguration and determines the reachability of neighboring nodes.

Navigate to **System > Network > Interfaces** and select the IPv6 interface you created earlier.

Set the **Administrative Access** to **Down**.

Return to the IPv6 interface and set the **Administrative Access** back to **Up**.

The screenshot shows the FortiGate configuration interface. On the left, the 'Firewall Objects' tree is expanded, showing 'Address' > 'Addresses'. On the right, the 'Create New' dropdown menu is open, showing 'IPv6 Address' selected. Below the menu, the 'Category' is set to 'IPv6 Address'. The 'Name' field is 'Port16', the 'IPv6 Address' field is '2001:db8::1/32', and 'Show in Address List' is checked. The 'Comments' field is empty. At the bottom, there are 'OK' and 'Cancel' buttons.

System  
Router  
Policy  
**Firewall Objects**

- Address
  - Addresses**
  - Groups
- Service

Create New Edit Address

- Address
  - IPv6 Address**
  - Multicast Address
  - Address Group
- LAN-Subnet
- Local LAN
- Port1-Subnet
- SSL-VPN-test
- SSLVPN\_TUNNEL\_ADDR1
- all

Category: ☐ Address ☒ IPv6 Address ☐ Multicast Address

Name: Port16

IPv6 Address: 2001:db8::1/32

Show in Address List: ☒

Comments: Write a comment... 0/255

OK Cancel

Administrative Status: ☐ Up ☒ Down

Administrative Status: ☒ Up ☐ Down



Alternatively, you can reboot the FortiGate device, or wait for the next router advertisement.

## Results

If you haven't done so already, connect a computer to the IPv6 interface you created.

On that computer, use the Command Prompt or Terminal, whichever is available, to view the IP configuration.

**Windows:** Enter `ipconfig` into the Command Prompt.

**Mac:** Enter `ifconfig` into Terminal.

You should see that an IPv6 address has been assigned using the prefix advertised on the connected IPv6 interface.

```
Ethernet adapter Local Area Connection :  
Connection-specific DNS Suffix . :  
IPv6 Address. . . . . : 2001:db8::44d2:ed61:9733:9253
```

# Authentication

Authentication, the act of confirming the identity of a person or device, is a key part of network security. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit enables controlled network access and applies authentication to users of security policies and VPN clients.

This section contains the following examples:

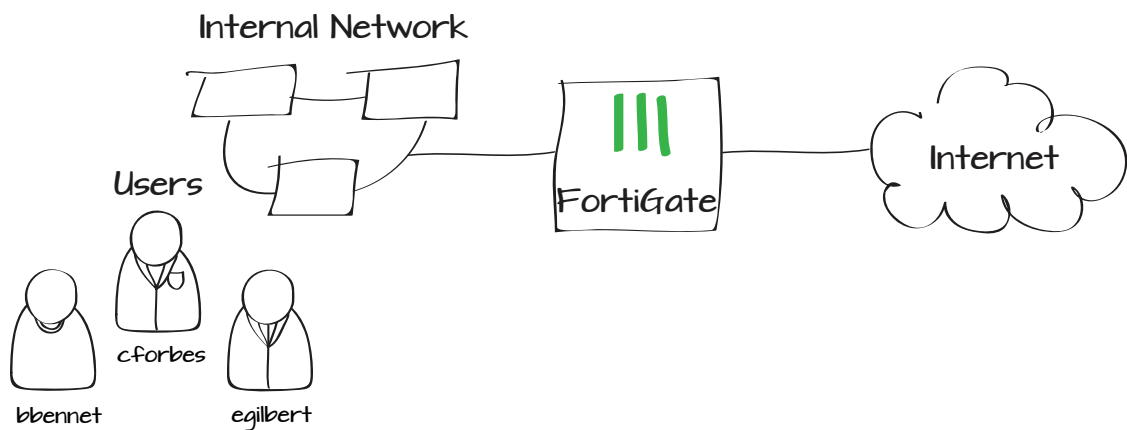
- [Identifying network users and applying web filters based on identity](#)
- [Controlling when specific types of devices can access the Internet](#)
- [Providing Single Sign-On for a Windows AD network with a FortiGate](#)
- [Providing Single Sign-On in advanced mode for a Windows AD network](#)
- [Providing Single Sign-On for Windows AD with LDAP](#)
- [Allowing Single Sign-On access with a FortiGate and a FortiAuthenticator](#)
- [Fortinet Single Sign-On in Polling Mode for a Windows AD network](#)
- [Preventing security certificate warnings when using SSL inspection](#)
- [Extra help: Certificates](#)
- [Adding FortiToken two-factor authentication to a user account](#)
- [Using two-factor authentication with IPsec VPN](#)
- [Using two-factor authentication with SSL VPN](#)
- [Authenticating SSL VPN users using LDAP](#)



# Identifying network users and applying web filters based on identity

This example uses an identity-based security policy to identify and monitor all users accessing the Internet through your FortiGate unit by requiring them to authenticate in order to connect. Different web filtering profiles will also be applied to traffic based on the user's credentials.

1. Creating users
2. Creating a user group
3. Creating a web filter profile
4. Configuring an identity-based security policy
5. Results



# Creating users

Go to **User & Device > User > User Definition**.

Using the **User Creation Wizard**, create three local users: *bbennet*, *cforbes*, and *egilbert*.

All three users now appear in the user list.

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

☒ Local User

☐ Remote RADIUS User

☐ Remote TACACS+ User

☐ Remote LDAP User

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

User Name

cforbes

Password

\*\*\*\*\*

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

Email Address

cforbes@example.com

☐ SMS

< Back

Next >

Cancel

1 Choose User Type

2 Specify Login Credential

3 Provide Contact Info

4 Provide Extra Info

☒ Enable

☐ Two-factor Authentication

☐ User Group

Click to set...

< Back

Done

Cancel

# Creating a user group

Go to **User & Device > User > User Groups**.

Create a new user group and add users bbennet and cforbes.

The user group now appears in the user group list.

Name

employees

Type

☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest

Members

bbennet

X

cforbes

X

Group Name	Group Type	Members	
FSSO_Guest_Users (0 Members)	Fortinet Single Sign-On (FSSO)		0
employees (2 Members)	Firewall	<div><div>bbennet</div><div>cforbes</div></div>	0

# Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**. The default web filter profile is shown, which will be later applied to traffic for members of the user group.

Create a new profile. Enable **FortiGuard Categories** and set the category **General Interest - Personal** to **Block**.

Name

restricted\_access

Comments

Write a comment...0/255

Inspection Mode

☒ Proxy ☐ Flow-based ☐ DNS

☒ FortiGuard Categories

Show All X

Local Categories

Potentially Liable

Adult/Mature Content

Bandwidth Consuming

Security Risk

General Interest - Personal

General Interest - Business

Unrated

Identifying network users and applying web filters based on identity

259

## Configuring an identity-based security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling your outgoing traffic and set **Policy Subtype** to **User Identity**.

Create two **Authentication Rules** that allow Internet access. For the first rule, set **Group(s)** to the user group. Enable **Web Filter** and set it to use the default profile.

For the second rule, set **User(s)** to egilbert. Enable **Web Filter** and set it to use the new profile.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input type="radio"/> Address <input checked="" type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	lan
Source Address	all
Outgoing Interface	wan1
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	
Destination Address	all
Group(s)	employees
User(s)	Click to add...
Schedule	always
Service	ALL
Action	ACCEPT
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="radio"/> AntiVirus	default
<input checked="" type="radio"/> Web Filter	default
Destination Address	all
Group(s)	Click to add...
User(s)	egilbert
Schedule	always
Service	ALL
Action	ACCEPT
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>Security Profiles</b>	
<input type="radio"/> AntiVirus	default
<input checked="" type="radio"/> Web Filter	restricted_access

# Results

When a user attempts to connect to the Internet, the authentication screen will appear. In order to get full Internet access, log in as user cforbes.

Browse to [www.ebay.com](http://www.ebay.com), a site that is in the **General Interest - Personal** category. Using this account, you can access the website.

Go to **User & Device > Monitor > Firewall**. The cforbes account appears on the firewall monitor list.

Select the account on the list and select **De-authenticate**. This will require you to enter the credentials again in order to continue browsing the Internet.

Log in again, this time using the egilbert account.

Browse to [www.ebay.com](http://www.ebay.com). Now that you are using the egilbert account, the website will be blocked.

**FORTINET®**

Authentication Required


Please enter your username and password to continue.


Username:

Password:

Continue

User Name	User Group	Duration	IP Address
cforbes	employees	0 day(s) 0 hour(s) 1 minute(s)	192.168.13.110

FortiGuard Web Filtering



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.  
URL: [www.ebay.com/](http://www.ebay.com/)  
Category: Shopping and Auction  
To have the rating of this web page re-evaluated [please click here](#).

Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click on the header row, enable the **User** column, and select **Apply** to view session information for each user.



You may be required to scroll down the menu in order to select **Apply**.

Select an entry for more information.

Date/Time	User	Destination	Security Action
12:54:05	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:04	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:04	cforbes	23.1.169.232 (gh.ebaystatic.com)	
12:54:04	cforbes	108.166.2.184 (www.innovatia.net)	
12:54:03	cforbes	142.166.163.53 (elearning1.innovatia.net)	
12:53:48	bbennet	199.27.72.196 (widgets.pinterest.com)	
12:53:47	bbennet	199.27.78.134 (mac-tuts.disqus.com)	
12:53:44	bbennet	66.211.178.172 (rover.ebay.com)	
12:53:44	bbennet	199.27.78.196 (a.ssl.fastly.net)	
12:53:44	bbennet	173.192.42.188 (disqus.com)	
12:52:54	egilbert	184.84.41.232 (e2405.b.akamaiedge.net)	✗
12:52:54	egilbert	66.211.178.172 (rover.ebay.com)	✗
12:52:54	egilbert	23.1.169.232 (gh.ebaystatic.com)	✗

Application Details	rover.ebay.com	Category Description	Shopping and Auction
Date/Time	08:21:57 (1382430117)	Destination	66.211.178.172 (rover.ebay.com)
Destination Country	United States	Dst Interface	wan1
Dst Port	80	Duration	11
Group	egilbert	Hostname	rover.ebay.com
Identity Index	2	Level	notice
Log ID	13	Policy ID	3
Protocol	6	Received	3152
Received Packets	6	Security Action	✗
Security Event	webfilter	Security Sub Type	ftgd-cat
Sent	1071	Sent / Received	1.05 KB / 3.08 KB
Sent Packets	5	Sequence Number	89431
Service	HTTP	Source	egilbert (192.168.13.110)
Source Country	Reserved	Src Interface	lan
Src NAT IP	172.20.120.236	Src NAT Port	61814
Src Port	61814	Status	close
Sub Type	forward	Threat	Shopping and Auction

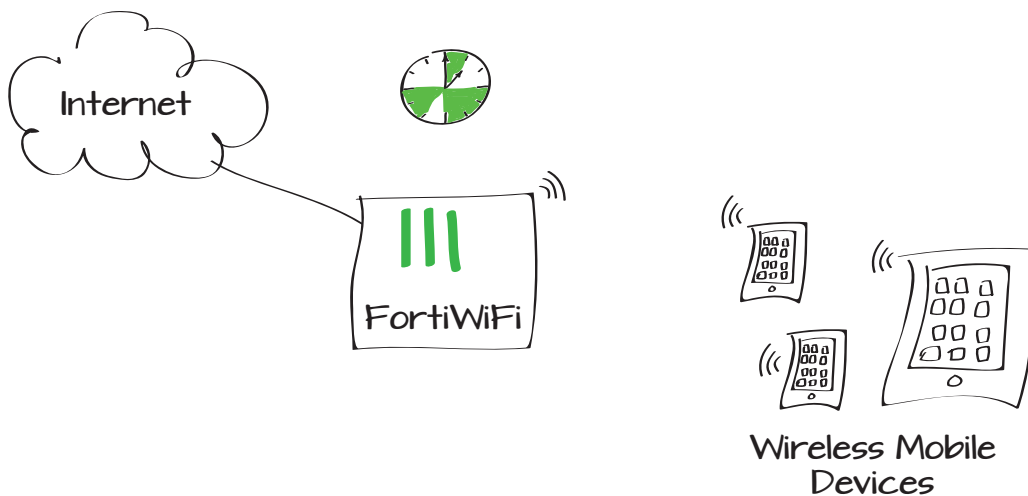
# Controlling when specific types of devices can access the Internet

In this example, a school does not allow Internet access to mobile devices between 9am - 12pm and 1pm - 3pm. To implement this, you create a device identity policy that permits Internet access for these devices before classes, at lunch time, and after classes. The school is open from 7am to 6pm.



In this example, a FortiWiFi unit is used. A similar method can be used to control access using a FortiAP and a FortiGate..

1. Creating the schedule
2. Creating the device policy
3. Configuring the authentication rule
4. Results



# Creating the schedules and schedule group

The schedule covers several periods. It is created by combining several schedules into a schedule group.

Go to **Firewall Objects > Schedule > Schedules**. Create recurring schedules for the before class (7-9am), lunch (12-1pm), and after class (3-6pm) periods.

Go to **Firewall Objects > Schedule > Groups**.

Create a group and add the schedules that you created before.

Name

before class

Day of the Week

☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday

Start Time

Hour 

07

 Minute 

00

Stop Time

Hour 

09

 Minute 

00

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will be during the next day.

OK

Cancel

Name

lunch

Day of the Week

☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday

Start Time

Hour 

12

 Minute 

00

Stop Time

Hour 

13

 Minute 

00

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will be during the next day.

OK

Cancel

Name

after class

Day of the Week

☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday

Start Time

Hour 

15

 Minute 

00

Stop Time

Hour 

18

 Minute 

00

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will be during the next day.

OK

Cancel

Group Name

non-class time

Available Schedules:

always

am\_lessons

pm\_lessons

weekend

Members:

after class

before class

lunch

OK

Cancel



# Creating the device policy

Go to **Policy > Policy > Policy** and create a **Device Identity** policy to control Internet access.

Create a new **Authentication Rule**. Set **Device** to include all mobile device types and set **Schedule** to the new schedule group.

## Results

When a mobile user connects during a time set matching the schedule group, they can surf the Internet

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic from these devices.

Policy Type

Firewall VPN

Policy Subtype

Address User Identity Device Identity

Incoming Interface

ednet (SSID: ednet)

Source Address

all

Outgoing Interface

wan1

Enable NAT

Use Destination Interface Address

Fixed Port

Use Dynamic IP Pool

Click to add...

Configure Authentication Rules

Create New Edit Delete

Destination Address	Device	Endpoint Compliance	Service	Schedule	Security	Traffic Shaping	Logging	Action
all	All	-	ALL	always				DENY

Destination Address

all

Device

Android Phone

Android Tablet

iPad

iPhone

Windows Phone

Windows Tablet

Compliant with FortiClient Profile

Schedule

non-class time

Service

ALL

Action

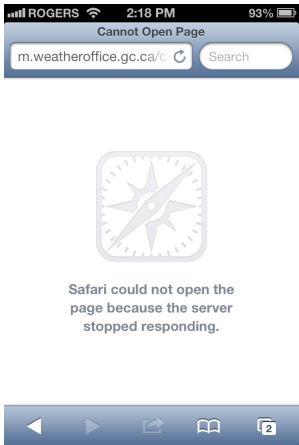
ACCEPT

Date/Time	Src	Device	Dst
17:00:48	20.10.10.40	Android Phone	8.8.8.8
15:00:28	20.10.10.40	Android Phone	216.250.166.65
12:58:38	20.10.10.40	Android Phone	65.55.172.252
12:48:26	20.10.10.41	iPad	17.172.208.30
7:44:46	20.10.10.41	iPad	8.8.8.8

Controlling when specific types of devices can access the Internet

265

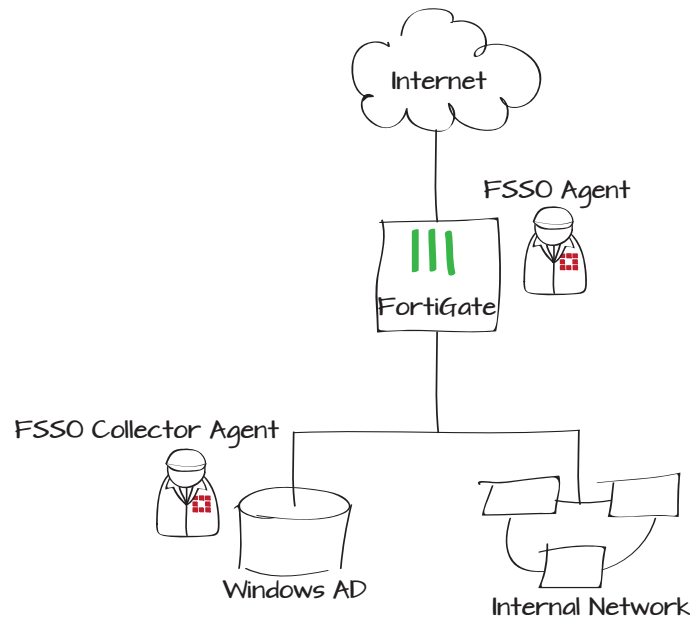
When the time in the schedule is reached, further surfing cannot continue. This does not appear in the logs, as only allowed traffic is logged.



# Providing Single Sign-On for a Windows AD network with a FortiGate

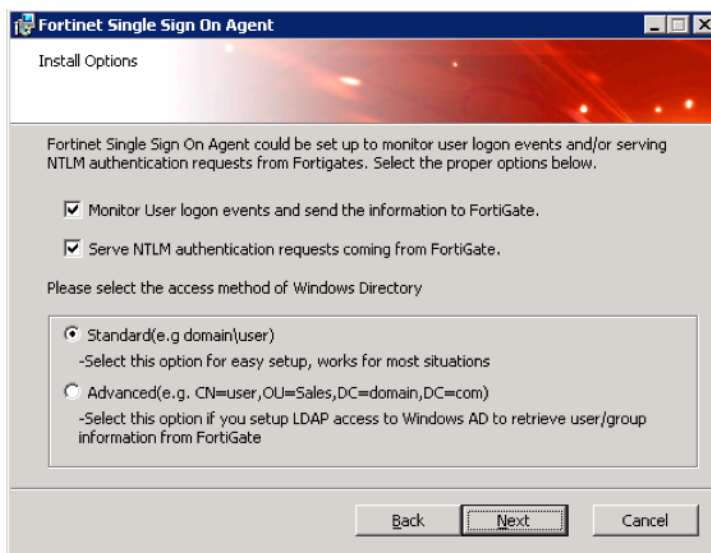
This example uses the Fortinet Single Sign-On (FSSO) Collector Agent to integrate a FortiGate unit into the Windows AD domain.

1. Installing the FSSO Collector Agent
2. Configuring the Single Sign-on Agent
3. Configuring the FortiGate unit to connect to the FSSO agent
4. Adding a FSSO user group
5. Adding a firewall address for the internal network
6. Adding a security profile that includes an authentication rule
7. Results

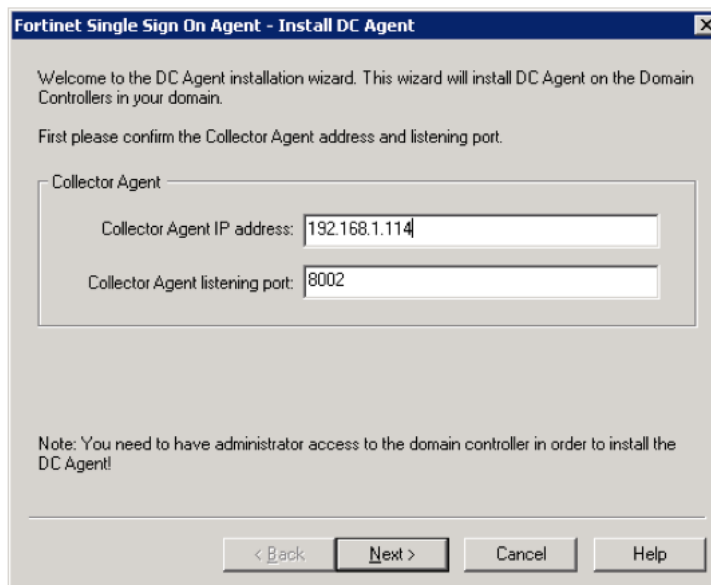


## Installing the FSSO Collector Agent

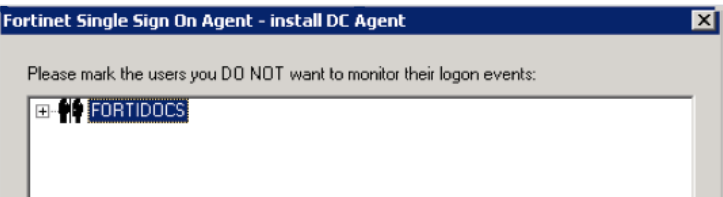
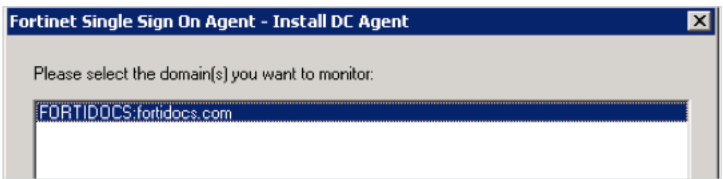
Run the setup for the Fortinet SSO Collector Agent. After logging in, configure the agent settings.



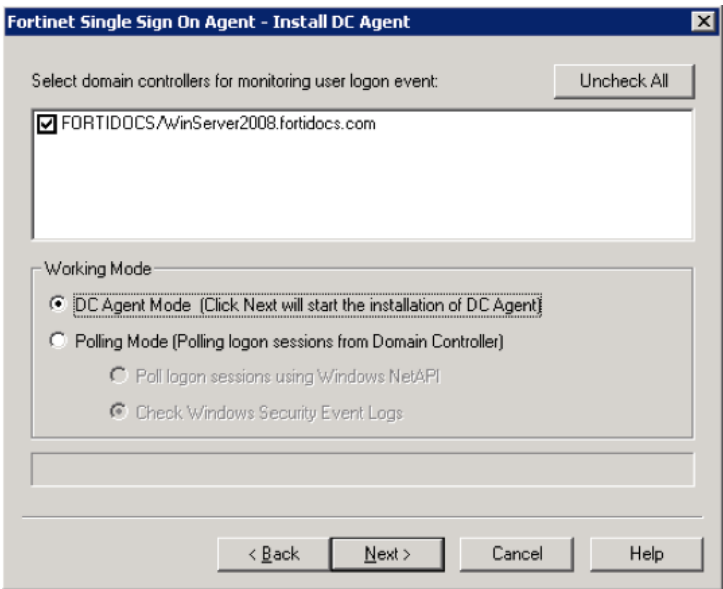
Add the Collector Agent address information.



Select the domains to monitor, and any users whose activity you do not wish to monitor.



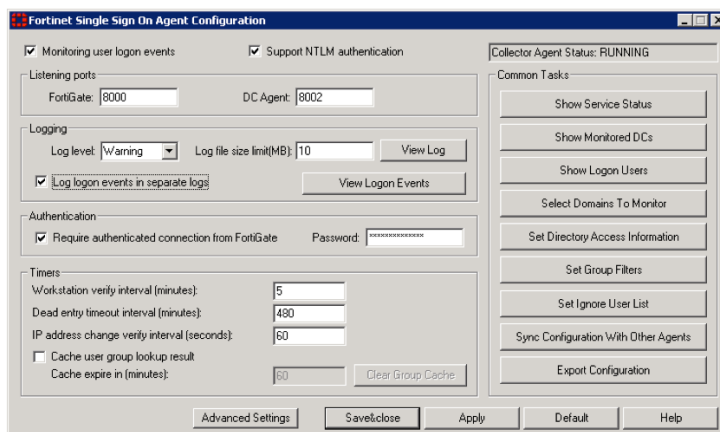
Set the working mode and complete the installation.



## Configuring the Single Sign-on Agent

If required, select Require authenticated connection from FortiGate, and add a password.

You will also enter this password when configuring the FSSO on the FortiGate unit.

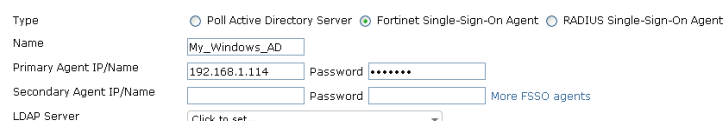


The screenshot shows the 'Fortinet Single Sign On Agent Configuration' window. It has several sections: 'Monitoring user logon events' with checkboxes for 'Monitoring user logon events' and 'Support NTLM authentication'; 'Listening ports' with 'FortiGate' set to 8000 and 'DC Agent' to 8002; 'Logging' with 'Log level' set to Warning, 'Log file size limit(MB)' set to 10, and a checkbox for 'Log logon events in separate logs'; 'Authentication' with a checkbox for 'Require authenticated connection from FortiGate' and a password field; 'Timers' with 'Workstation verify interval (minutes)' set to 5, 'Dead entry timeout interval (minutes)' set to 480, 'IP address change verify interval (seconds)' set to 60, and a checkbox for 'Cache user group lookup result'; and a 'Common Tasks' panel on the right with buttons for 'Show Service Status', 'Show Monitored DCs', 'Show Logon Users', 'Select Domains To Monitor', 'Set Directory Access Information', 'Set Group Filters', 'Set Ignore User List', 'Sync Configuration With Other Agents', and 'Export Configuration'. At the bottom are buttons for 'Advanced Settings', 'Save/Close', 'Apply', 'Default', and 'Help'.

## Configuring the FortiGate unit to connect to the FSSO agent

On the FortiGate unit, go to **User & Device > Authentication > Single Sign-On**.

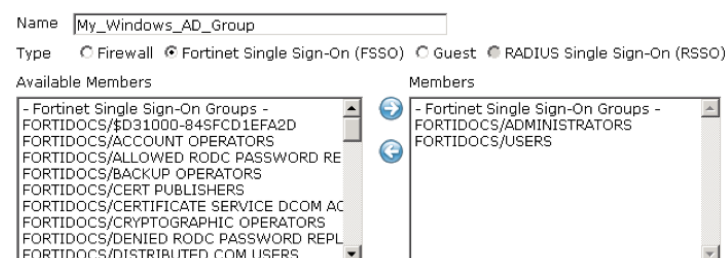
Enter this password used configuring the FSSO on the FortiGate unit in the previous step.



The screenshot shows the 'Single Sign-On' configuration window on the FortiGate. It has radio buttons for 'Poll Active Directory Server', 'Fortinet Single-Sign-On Agent' (which is selected), and 'RADIUS Single-Sign-On Agent'. Below are fields for 'Name' (My\_Windows\_AD), 'Primary Agent IP/Name' (192.168.1.114), 'Secondary Agent IP/Name', and 'LDAP Server' (Click to set...). There are also password fields for the primary and secondary agents. A link 'More FSSO agents' is visible on the right.

## Adding a FSSO user group

On the FortiGate unit, go to **User & Device > User > User Groups**.



The screenshot shows the 'User Groups' configuration window on the FortiGate. It has a 'Name' field (My\_Windows\_AD\_Group) and radio buttons for 'Firewall', 'Fortinet Single Sign-On (FSSO)' (which is selected), 'Guest', and 'RADIUS Single Sign-On (RSSO)'. Below are two list boxes: 'Available Members' and 'Members'. The 'Available Members' list includes various FortiGate system groups like 'FORTIDOCs/\$D31000-845FCD1EFA2D', 'FORTIDOCs/ACCOUNT OPERATORS', etc. The 'Members' list is currently empty.

# Adding a firewall address for the internal network

Go to **Firewall Objects > Address > Addresses**.

# Adding a security profile that includes an authentication rule

Go to **Policy > Policy > Policy**.

Add an accept user identity security policy and add the new FSSO group.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

Write a comment...

0/255

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☐ Address ☒ User Identity ☐ Device Identity

Incoming Interface

port1

Source Address

Local LAN

Outgoing Interface

wan1

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool 

Click to add...

☐ Use Central NAT Table

☐ Enable Web cache

☐ Enable WAN Optimization

Configure Authentication Rules

Create New Edit Delete

User/Group	Destination Address	Service	Schedule	UTM Security	Traffic Shaping
My_Windows_AD_Group	all	ALL	always	-	
ANY	all	ALL	always	-	

☐ Skip this policy for unauthenticated user

☐ Disclaimer

☐ Customize Authentication Messages

Results

Go to **Log & Report > Traffic Log > Forward Traffic**. As users log into the Windows AD system, the FortiGate collects their connection information.

Select an entry for more information.

Date/Time	Src	Device	D
15:49	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	204.246.169.91 (cont
15:45	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	74.121.50.17 (www.p
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt

Dst	204.246.169.91 (content.mkt931.com)	Virtual Domain	root
Received	92	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	292 B / 92 B
Device Type	Windows PC	Duration	10
Sent	292	Src NAT Port	9803
Application Details		Group	My_Windows_AD_Group
Device	00:0c:29:4b:d7:cc	Service	HTTP
Protocol	6	byod_name	
User	ADMINISTRATOR	Destination Country	United States
Identity Index	1	Dst Port	80
roll	65372	Status	close
Timestamp	Tue May 7 15:59:49 2013	Tran Display	snat
OS Name	Windows	Sequence Number	1607872
Policy ID	9	Src Interface	port1
Src	ADMINISTRATOR (192.168.1.114)	Sent Packets	7
OS Version	Vista	Level	notice
Src Port	9803	Log ID	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	15:59:49 (Tue May 7 15:59:49 2013)
Dst Interface	wan1		

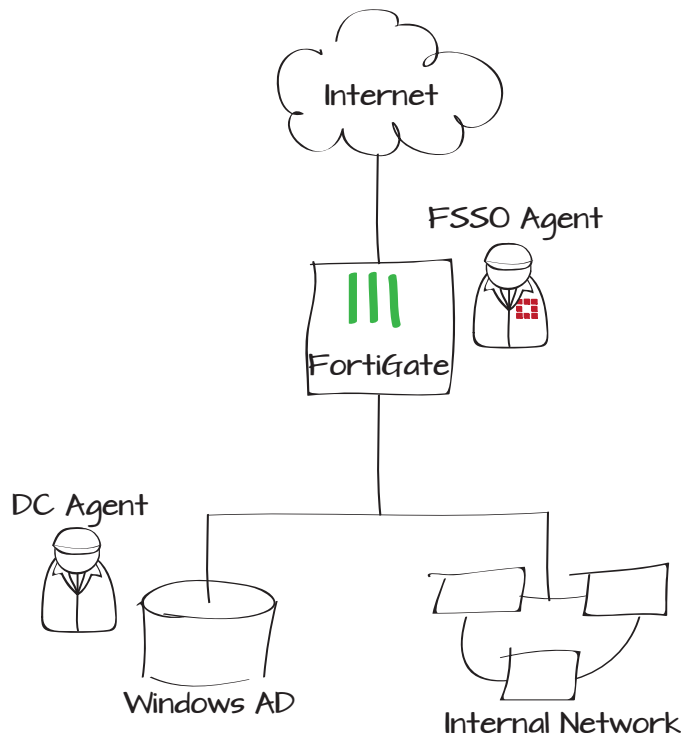
Dst	207.46.206.78 (mscr.microsoft.com)	Virtual Domain	root
Received	3202	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	609 B / 3.13 KB
Device Type	Windows PC	Duration	5
Sent	609	Src NAT Port	50608
Application Details		Group	My_Windows_AD_Group
Device	Lab test system 2	Service	HTTP
Protocol	6	byod_name	Lab test system 2
User	TWHITE	Destination Country	United States
Identity Index	1	Dst Port	80
roll	65372	Status	close
Timestamp	Tue May 7 15:59:07 2013	Tran Display	snat
OS Name	Windows	Sequence Number	1607691
Policy ID	9	Src Interface	port1
Src	TWHITE (192.168.1.116)	Sent Packets	7
OS Version	7	Level	notice
Src Port	50608	Log ID	13
Sub Type	forward	Threat	
Received Packets	7	Date/Time	15:59:07 (Tue May 7 15:59:07 2013)
Dst Interface	wan1		



# Providing Single Sign-On in advanced mode for a Windows AD network

Using Fortinet Single Sign-On, the FortiGate unit automatically authenticates any user that successfully logs into Windows. The Domain Controller agent Advanced mode has the advantage of supporting nested or inherited user groups. If Standard mode is used, the FortiGate unit can authenticate only users who are a direct member of a group.

1. Configuring the DC agent for Advanced mode
2. Configuring the DC agent as an FSSO agent
3. Creating an FSSO user group
4. Creating an identity-based security policy
5. Results

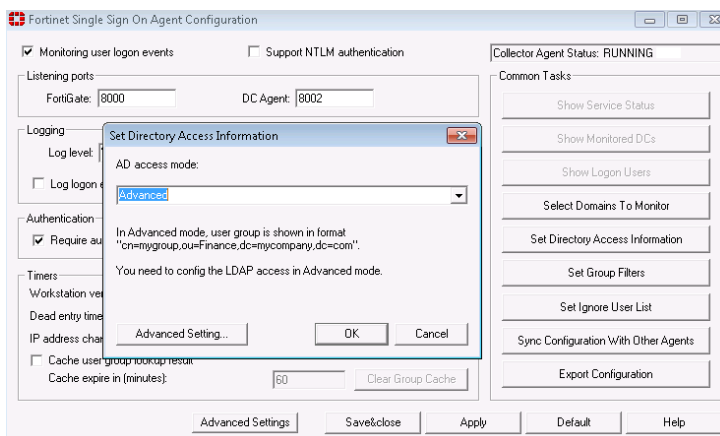


## Configuring the DC agent for Advanced mode

Log on to the Windows server where the DC agent is installed. Go to **All Programs > FortiNet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.

Select **Directory Access Information** and set **AD Access mode** to Advanced.

The rest of the configuration is done on the FortiGate unit.



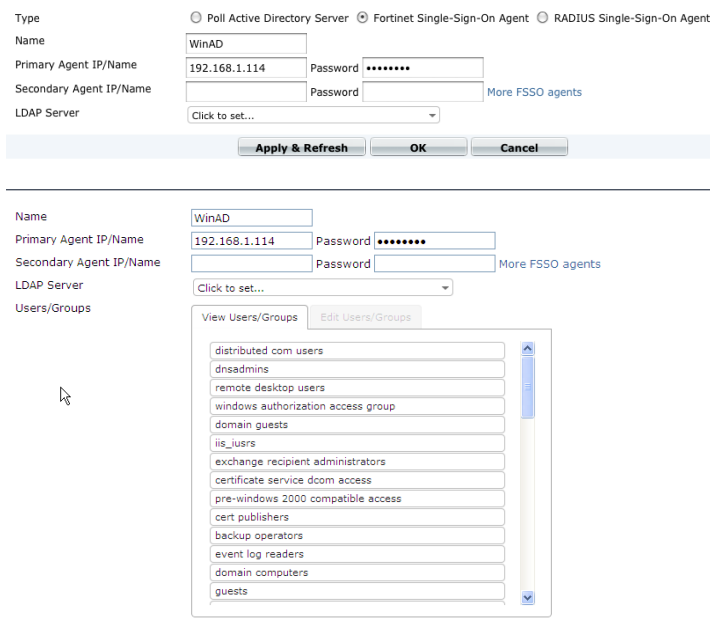
## Configuring the FSSO agent

Go to **User & Device > Authentication > Single Sign-On** to enter the information the FortiGate unit needs to access the DC agent.

After you select **Apply & Refresh**, the Windows AD groups are listed. This confirms that the FortiGate unit can communicate with the DC agent.



On a Windows AD network with a large number of groups, the FortiGate unit's performance might be affected by the volume of user logon information it receives. Use the **Set Group Filters** function of the DC agent to send information only for the groups you intend to authenticate.



# Creating an FSSO user group

Select the Windows AD groups to include in the FortiGate FSSO user group.

# Creating an identity-based security policy

Create an identity-based security policy that uses the FSSO user group that you created.

# Results

The Windows AD user, having authenticated at logon, does not have to authenticate again to connect to the Internet.

Name

My\_Windows\_AD\_Group

Type

☐ Firewall

☒ Fortinet Single Sign-On (FSSO)

☐ Guest

☐ RADIUS Single Sign-On (RSSO)

Available Members

- Fortinet Single Sign-On Groups -

CN=ACCOUNT OPERATORS,CN=BUILTIN,DC=FO

CN=ADMINISTRATORS,CN=BUILTIN,DC=FOR

CN=ALLOWED RODC PASSWORD REPLICATION

CN=BACKUP OPERATORS,CN=BUILTIN,DC=FO

CN=CERT PUBLISHERS,CN=USERS,DC=FOR

CN=CERTIFICATE SERVICE DCOM ACCESS,CN

CN=CRYPTOGRAPHIC OPERATORS,CN=BUILTIN

CN=DENIED RODC PASSWORD REPLICATION C

CN=DISTRIBUTED COM USERS,CN=BUILTIN,D

Members

- Fortinet Single Sign-On Groups -

CN=DOMAIN USERS,CN=USERS,DC=FORTIDO

OK

Cancel

Policy Type

☒ Firewall

☐ SSL-VPN

Policy Subtype

☐ Address

☒ User Identity

☐ Device Identity

Incoming Interface

port1

Source Address

Local LAN

Outgoing Interface

wan1

☒ Enable NAT

☐ Use Destination Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

Configure Authentication Rules

Create New

Edit

Delete

User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
My_Windows_AD_Group	all	ALL	always	-			ACCEPT
ANY	all	ALL	always	-			DENY

☐ Skip this policy for unauthenticated user

☐ Disclaimer

☐ Customize Authentication Messages

Comments

Write a comment...

0/1023

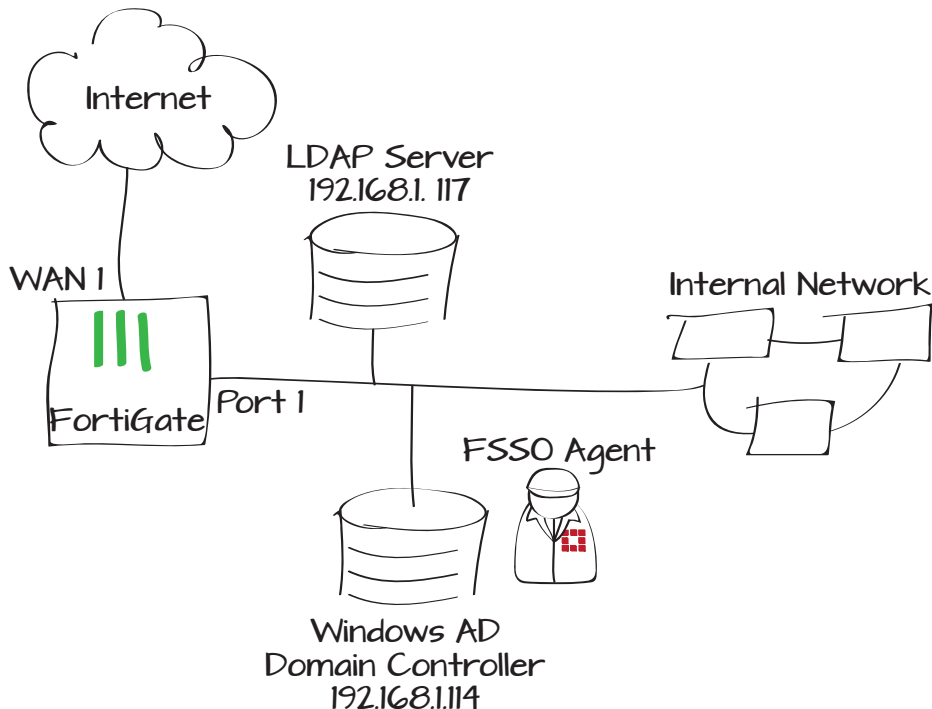
OK

Cancel

# Providing Single Sign-On for Windows AD with LDAP

A logged-on Windows user can be automatically authenticated on a FortiGate unit through Fortinet Single Sign-On. Some Windows AD systems use an external LDAP server. FSSO can also accommodate this configuration.

1. Configuring access to the LDAP server
2. Configuring the DC agent as an FSSO agent
3. Configuring a group filter on the FSSO agent
4. Creating an FSSO user group and adding AD user groups
5. Creating a security policy to allow the FSSO user group access
6. Results



## Configuring access to the LDAP server

Go to **User & Device > Authentication > LDAP Servers** and enter the information needed to connect the FortiGate unit to the external LDAP server.

This screenshot shows the configuration window for an LDAP server. The fields are filled with the following values:

Field	Value
Name	FAC_LDAP
Server Name/IP	192.168.1.117
Server Port	389
Common Name Identifier	uid
Distinguished Name	dc=fortidocs,dc=com
Bind Type	Simple (selected)
User DN	uid=test,ou=techdoc,c
Password	*****
Secure Connection	<input type="checkbox"/>

At the bottom, there is a 'Test' button and 'OK' and 'Cancel' buttons.

## Configuring the DC agent as an FSSO agent

Go to **User & Device > Authentication > Single Sign-On** to enter the information the FortiGate unit needs to access the DC agent.

Select the LDAP Server. In Users/Groups use the Edit Users/Groups tab to select user groups from the LDAP tree.

This screenshot shows the configuration window for a Single Sign-On (FSSO) agent. The fields are filled with the following values:

Field	Value
Name	WinAD
Primary Agent IP/Name	192.168.1.114
Secondary Agent IP/Name	
LDAP Server	FAC_LDAP (selected from dropdown)
Users/Groups	techdoc (selected from dropdown)

There are 'View Users/Groups' and 'Edit Users/Groups' tabs. The 'Edit Users/Groups' tab is active, showing a search box with 'techdoc' entered. At the bottom, there are 'OK' and 'Cancel' buttons.

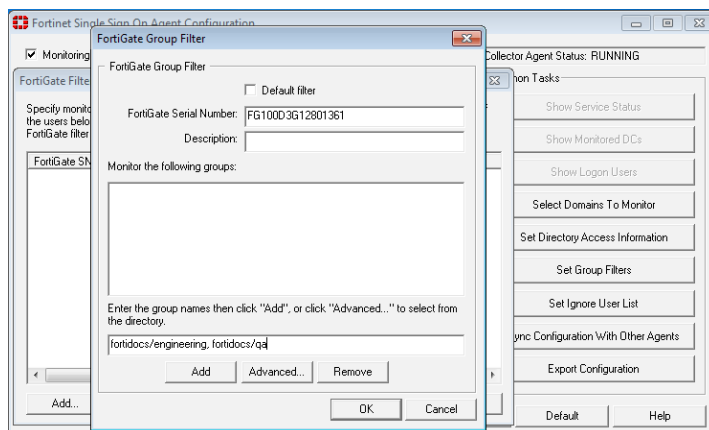
## Configuring a group filter on the FSSO agent

Log on to the Windows server where the DC agent is installed. Go to **All Programs > FortiNet > Fortinet Single Sign On Agent > Configure Fortinet Single Sign On Agent**.

Select **Set Group Filters**. Select **Add**. Enter the FortiGate unit serial number and specify which user groups the DC agent should monitor for the FortiGate unit. Select **Add** again.

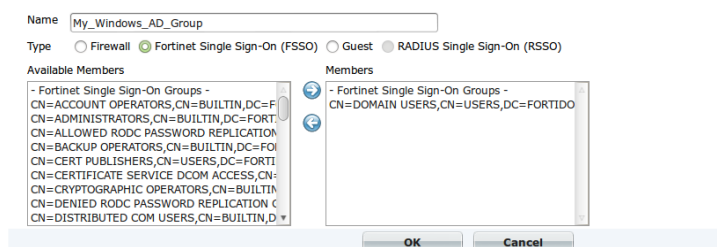


To avoid adversely affecting the FortiGate unit's performance, configure the filter to send information only for the groups you intend to authenticate.



## Creating an FSSO user group and adding AD user groups

Go to **User & Device > User > User Groups**. Create a Fortinet Single Sign-On group and select which Windows AD groups to include as members.



# Creating a security policy to allow the FSSO user group access

Create identity-based security policies that use the FSSO user group that you created.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

☒ Enable NAT

☐ Use Destination Interface Address

☐ Use Dynamic IP Pool

☐ Fixed Port

Click to add...

☐ Firewall

☐ SSL-VPN

☐ Address

☒ User Identity

☐ Device Identity

port1

LocalLAN

wan1

Create New

User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
My_Windows_AD_Group	all	ALL	always	-			✓ ACCEPT
ANY	all	ALL	always	-			✗ DENY

☐ Skip this policy for unauthenticated user

☐ Disclaimer

☐ Customize Authentication Messages

Comments

Write a comment...

0/1023

OK

Cancel

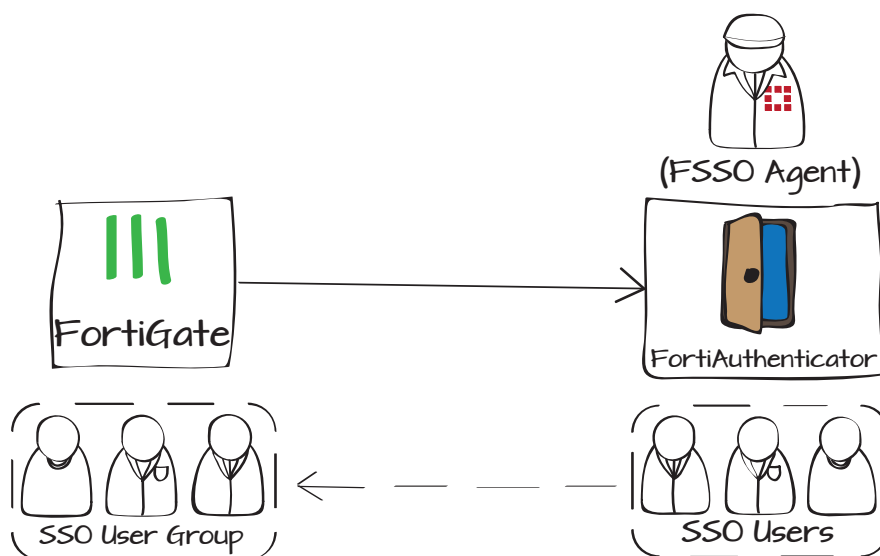
## Results

The Windows AD user, having authenticated at logon, does not have to authenticate again to connect to the Internet.

# Allowing Single Sign-On access with a FortiGate and a FortiAuthenticator

This example illustrates how to configure Single Sign-On (SSO) using a FortiGate and FortiAuthenticator, with the FortiAuthenticator unit acting as the SSO Agent, verifying and maintaining user login information. Users can then log in once when connecting to the internal network behind the FortiGate, and be automatically logged into servers and services that support SSO.

1. Configuring polling on the FortiAuthenticator
2. Adding a FortiAuthenticator to the FortiGate unit
3. Creating the FSSO user group
4. Creating a security policy
5. Results





## Configuring polling on the FortiAuthenticator

In the FortiAuthenticator interface, go to **SSO & Dynamic Policies > SSO > Options**.

In the **FortiGate** section, the Listening Port should be 8000, unless the FortiGate's default port mapping has been changed.

Select **Enable Authentication**, and enter the **Secret Key**, which you will use when configuring the FSSO Agent on the FortiGate.

If you are using an external SSO service, such as Windows AD or a remote LDAP server, enable it in the the **Fortinet Single Sign-On (FSSO)** section.

Go to **SSO & Dynamic Policies > SSO > Login Portal** and **Enable SSO Portal**. Ensure **Local users** is enabled, and disable **Remote users from an LDAP server**.

Then go to **SSO & Dynamic Policies > SSO > FortiGate Group Filtering**.

Create a new **FortiGate Group Filter**, entering the FortiGate's IP/hostname.

Enable **Forward FSSO information for users from the following subset of groups only** and move the groups you'd like to send to the FortiGate from **Available** to **Selected**. Select **OK** to save the filter.

The screenshot displays the FortiAuthenticator configuration interface, specifically the 'FortiGate' and 'Fortinet Single Sign-On (FSSO)' sections.

**FortiGate Section:**

- Listening port:** 8000
- Login expiry:** 480 minutes
- ☒ **Enable authentication**
- Secret key:** [Redacted]

**Fortinet Single Sign-On (FSSO) Section:**

- Log level:** Info
- ☐ **Enable Windows Active Directory domain controller polling**
- ☐ **Enable RADIUS Accounting SSO clients**
- ☐ **Enable FortiClient SSO Mobility Agent Service**
- ☐ **Restrict auto-discovered domain controllers to configured domain controllers**
- Restart SSO service** button

**Enable SSO Portal Section:**

- ☒ **Enable SSO Portal**
- Enable SSO for the following sets of users:**
  - ☒ **Local users**
    - ☒ **All local users**
    - ☐ **Local users from selected groups only**
  - ☐ **Remote users from an LDAP server:** [ Please Select ]

**Fortinet Single Sign-On (FSSO) Section (Group Filtering):**

- ☒ **Forward FSSO information for users from the following subset of groups only:**
- Available sso groups:** [Search bar, list of groups]
- Selected sso groups:** [Search bar, list of groups, "fsso\_sample\_group" is selected]

## Adding a FortiAuthenticator to the FortiGate unit

In the FortiGate interface, go to **User & Device > Authentication > Single Sign-On**, and select **Create New**.

For the **Type**, select Fortinet Single Sign-On Agent. Enter a **Name** for the FortiAuthenticator unit.

Enter the IP address of the FortiAuthenticator as the **Primary Agent IP/Name**, and enter the secret key as the **Password**.

Select **Apply & Refresh**, and wait a minute for the FortiAuthenticator to connect to the FortiGate and download user group information.

Name	<input type="text" value="My_FAC"/>		
Primary Agent IP/Name	<input type="text" value="192.168.1.117"/>	Password	<input type="password" value="....."/>
Secondary Agent IP/Name	<input type="text"/>	Password	<input type="password"/>
LDAP Server	<input type="text" value="Click to set..."/>		
Users/Groups	<div><input type="button" value="View Users/Groups"/> <input type="button" value="Edit Users/Groups"/></div> <div><input type="text" value="FSSO_SAMPLE_GROUP"/></div>		

## Creating the FSSO user group

You cannot directly use the user groups imported from FortiAuthenticator in firewall policies, so you will need to create FortiGate user groups to represent the FortiAuthenticator groups. Go to **User & Device > User > User Groups**, and create a new FSSO user group.

The **Members** list will be populated with the FortiAuthenticator's user groups. Select the imported groups to add them to the FortiGate group's **Members** list.

Name	<input type="text" value="FSSO_users_group"/>		
Type	<input type="radio"/> Firewall <input checked="" type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest		
Members	<div><input type="button" value="FSSO_SAMPLE_GROUP"/> <input type="button" value="X"/> <input type="button" value="+"/></div>		

# Creating a security policy

Now, create a security policy to handle SSO user traffic, so it can be easily identified in logs and reports. Go to **Policy > Policy > Policy**, and create a new policy, setting the **Policy Subtype** to **User Identity**.

Multiple **Authentication Rules** can be created for different groups of SSO users that require different access and supervision.

## Results

With the identity-based policy being the only policy connecting the internal network to the internet, users on the internal network will not be able to access the internet without authenticating.

To connect to the internet, users must navigate in a browser to the FortiAuthenticator's IP. Users will then log into the FortiAuthenticator as an admin would, but will only have access to their user account settings in the FAC interface.

Once the user has logged in, the FortiAuthenticator retains their user information for a time specified in the SSO Portal settings. They will have access to the internet, and to any other services or servers on the internal network configured to use SSO with the FortiAuthenticator.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input type="radio"/> Address <input checked="" type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	port1
Source Address	all
Outgoing Interface	wan1
<input checked="" type="checkbox"/> Enable NAT	
Destination Address	all
Group(s)	FSSO_users_group
User(s)	Click to add...
Schedule	always
Service	ALL
Action	ACCEPT

Login

Username: twwhite

Password: .....

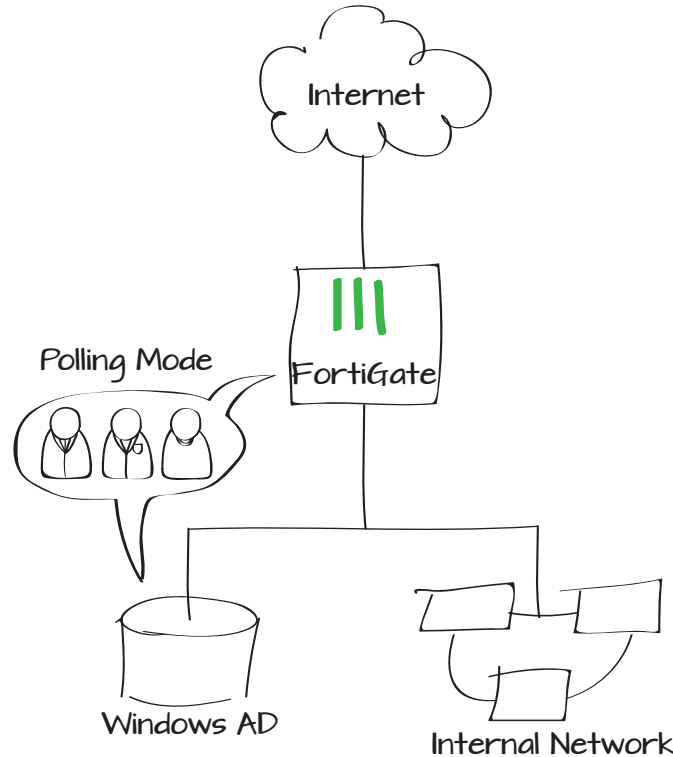
Login

[Forgot my password](#)

# Fortinet Single Sign-On in Polling Mode for a Windows AD network

This example uses Active Directory Polling to establish Fortinet Single Sign-On (FSSO) for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a Collector Agent running on the Windows AD Domain to act as an intermediary between the FortiGate and the domain.

1. Adding the LDAP Server to the FortiGate
2. Configuring the FortiGate unit to poll the Active Directory
3. Adding an FSSO user group
4. Adding a firewall address for the internal network
5. Adding a security policy that includes an authentication rule
6. Results



# Adding the LDAP Server to the FortiGate

In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**. Add your LDAP server details.

# Configuring the FortiGate unit to poll the Active Directory

Next, go to **User & Device > Authentication > Single Sign-On**.

For the **Type**, select **Poll Active Directory Server**. Enter the IP, username and password, and select the LDAP server you added previously. Ensure **Enable Polling** is checked.

# Adding an FSSO user group

Go to **User & Device > User > User Groups**, and add the desired AD member groups to the group.

Name	<input type="text" value="FAC_LDAP"/>
Server IP/Name	<input type="text" value="192.168.1.117"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="uid"/>
Distinguished Name	<input type="text" value="dc=fortidocs,dc=com"/>
Bind Type	<input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
User DN	<input type="text" value="ou=techdoc,dc=fortidocs,dc=com"/>
Password	<input type="password" value="....."/>

Type	<input checked="" type="radio"/> Poll Active Directory Server <input type="radio"/> Fortinet Single-Sign-On Agent <input type="radio"/>
Server IP/Name	<input type="text" value="192.168.1.117"/>
User	<input type="text" value="Example_Admin"/>
Password	<input type="password" value="....."/>
LDAP Server	<input type="text" value="FAC_LDAP"/>
Enable Polling	<input checked="" type="checkbox"/>
Users/Groups	<div><div>View Users/Groups</div><div>Edit Users/Groups</div><div><div>DC=fortidocs,DC=com</div></div></div>

Name <input type="text" value="My_Windows_AD_Group"/>	
Type <input type="radio"/> Firewall <input checked="" type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input type="radio"/> RADIUS Single Sign-On (RSSO)	
Available Members	Members
<div><div>- Fortinet Single Sign-On Groups - FORTIDOC/\$D31000-845FCD1EFA2D FORTIDOC\$/ACCOUNT OPERATORS FORTIDOC\$/ALLOWED RODC PASSWORD RE FORTIDOC\$/BACKUP OPERATORS FORTIDOC\$/CERT PUBLISHERS FORTIDOC\$/CERTIFICATE SERVICE DCOM AC FORTIDOC\$/CRYPTOGRAPHIC OPERATORS FORTIDOC\$/DENIED RODC PASSWORD REPL FORTIDOC\$/DISTRIBUTED COM USERS</div></div>	<div><div>- Fortinet Single Sign-On Groups - FORTIDOC\$/ADMINISTRATORS FORTIDOC\$/USERS</div></div>

# Adding a firewall address for the internal network

Go to **Firewall Objects > Address > Addresses**, and create an internal network address to be used by the policy.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

Write a comment...

0/255

# Adding a security policy that includes an authentication rule

Go to **Policy > Policy > Policy**.

Create a **User Identity** policy and add an authentication rule to allow your FSSO group to access the internet.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☐ Address ☒ User Identity ☐ Device Identity

Incoming Interface

port1

Source Address

Local LAN

Outgoing Interface

wan1

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool 

Click to add...

☐ Use Central NAT Table

☐ Enable Web cache

☐ Enable WAN Optimization

## Configure Authentication Rules

Create New

Edit

Delete

User/Group	Destination Address	Service	Schedule	UTM Security	Traffic Shaping
My_Windows_AD_Group	all	ALL	always	-	
ANY	all	ALL	always	-	

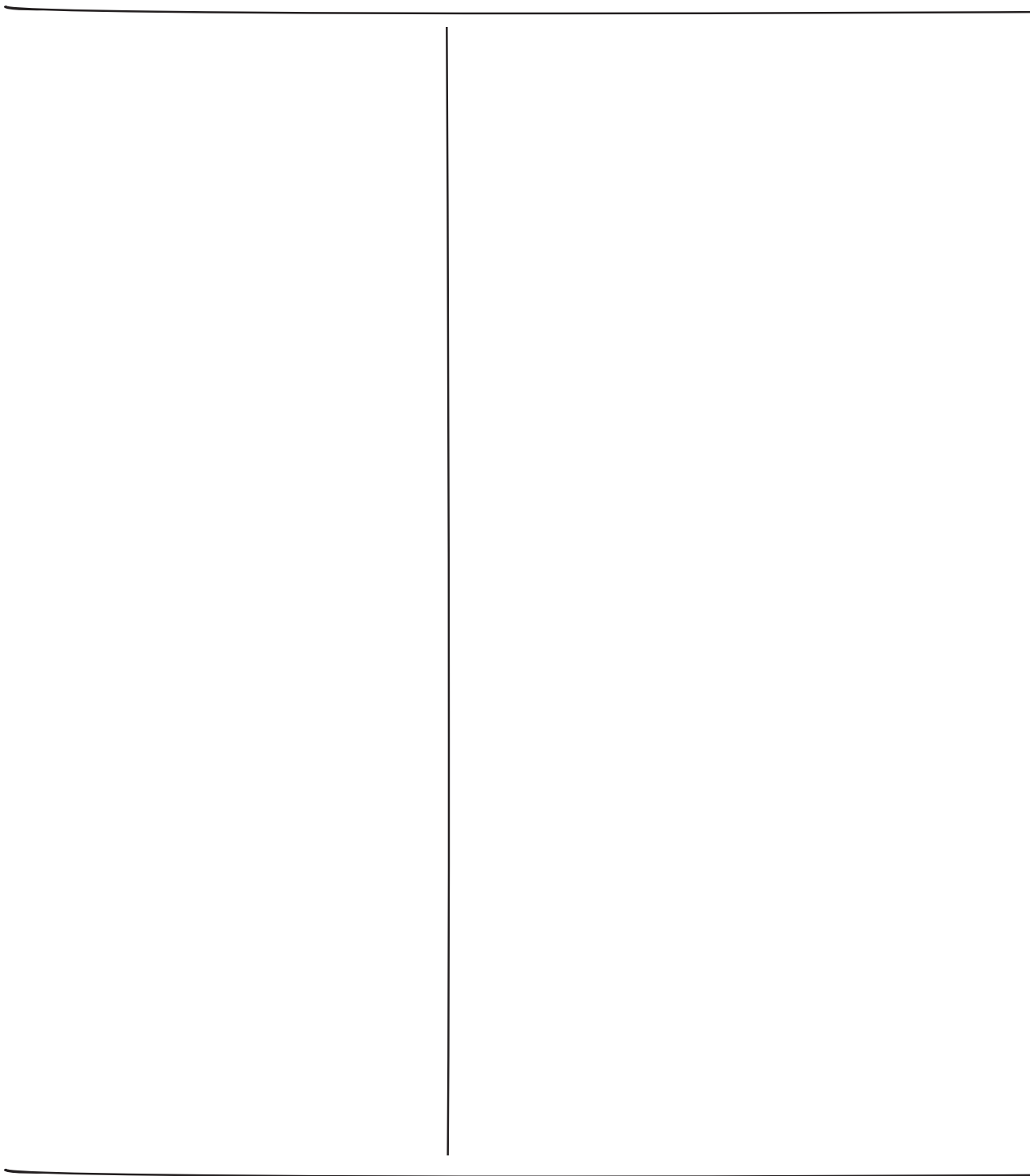
- ☐ Skip this policy for unauthenticated user
- ☐ Disclaimer
- ☐ Customize Authentication Messages

# Results

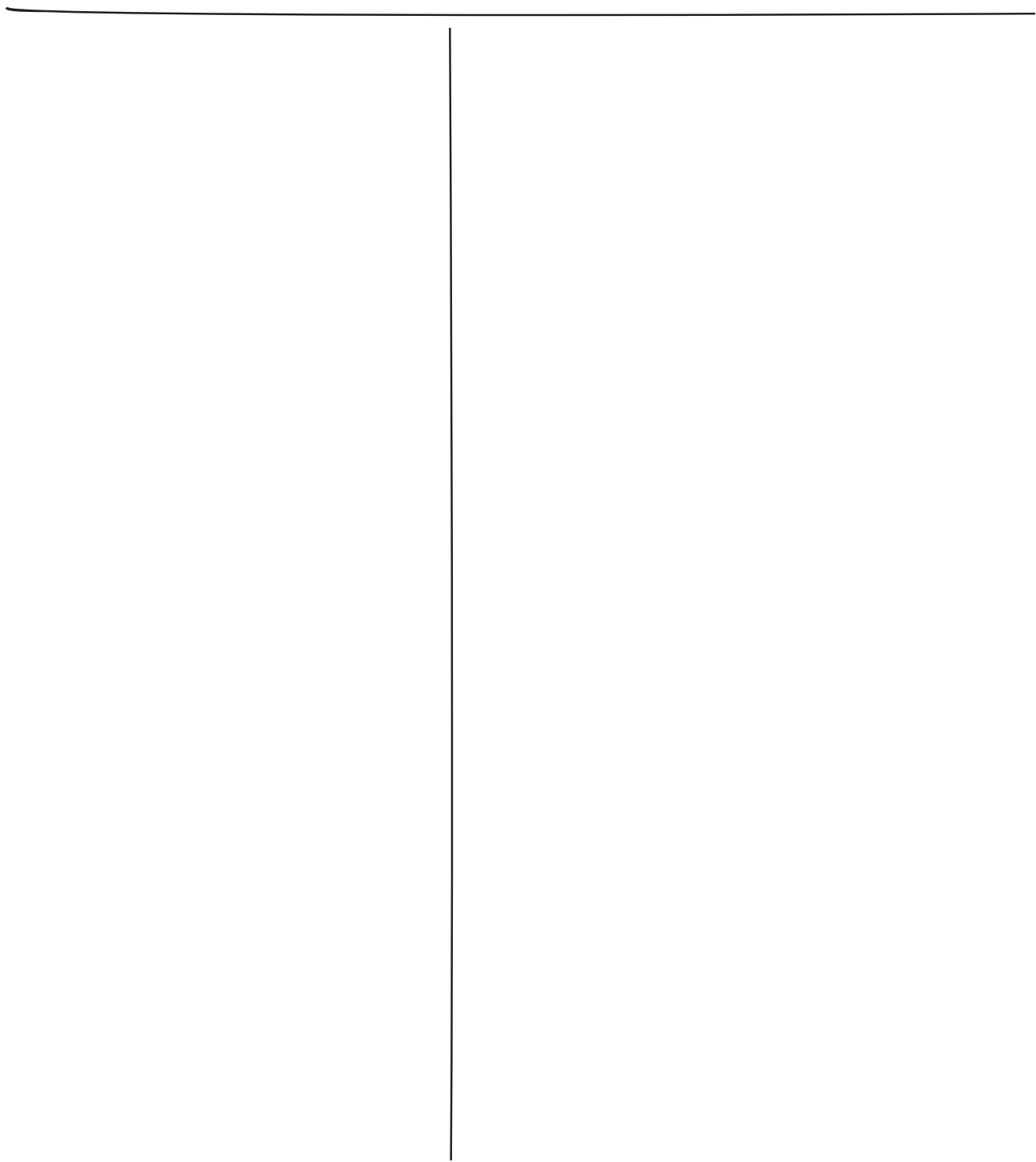
Go to **Log & Report > Traffic Log > Forward Traffic**. When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

Select an entry for more information.

Date/Time	Src	Device	Dst
15:49	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	204.246.169.91 (content.mkt931.com)
15:45	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	74.121.50.17 (www.p...
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr...
15:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscr...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...
15:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt...
Dst	204.246.169.91 (content.mkt931.com)	Virtual Domain	root
Received	92	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	292 B / 92 B
Device Type	Windows PC	Duration	10
Sent	292	Src NAT Port	9803
Application Details		Group	My_Windows_AD_Group
Device	00:0c:29:4b:d7:cc	Service	HTTP
Protocol	6	byod_name	
User	ADMINISTRATOR	Destination Country	United States
Identity Index	1	Dst Port	80
roll	65372	Status	close
Timestamp	Tue May 7 15:59:49 2013	Tran Display	snat
OS Name	Windows	Sequence Number	1607872
Policy ID	9	Src Interface	port1
Src	ADMINISTRATOR (192.168.1.114)	Sent Packets	7
OS Version	Vista	Level	notice
Src Port	9803	Log ID	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	15:59:49 (Tue May 7 15:59:49 2013)
Dst Interface	wan1		
Dst	207.46.206.78 (mscr.microsoft.com)	Virtual Domain	root
Received	3202	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	609 B / 3.13 KB
Device Type	Windows PC	Duration	5
Sent	609	Src NAT Port	50608
Application Details		Group	My_Windows_AD_Group
Device	Lab test system 2	Service	HTTP
Protocol	6	byod_name	Lab test system 2
User	TWHITE	Destination Country	United States
Identity Index	1	Dst Port	80
roll	65372	Status	close
Timestamp	Tue May 7 15:59:07 2013	Tran Display	snat
OS Name	Windows	Sequence Number	1607691
Policy ID	9	Src Interface	port1
Src	TWHITE (192.168.1.116)	Sent Packets	7
OS Version	7	Level	notice
Src Port	50608	Log ID	13
Sub Type	forward	Threat	
Received Packets	7	Date/Time	15:59:07 (Tue May 7 15:59:07 2013)
Dst Interface	wan1		



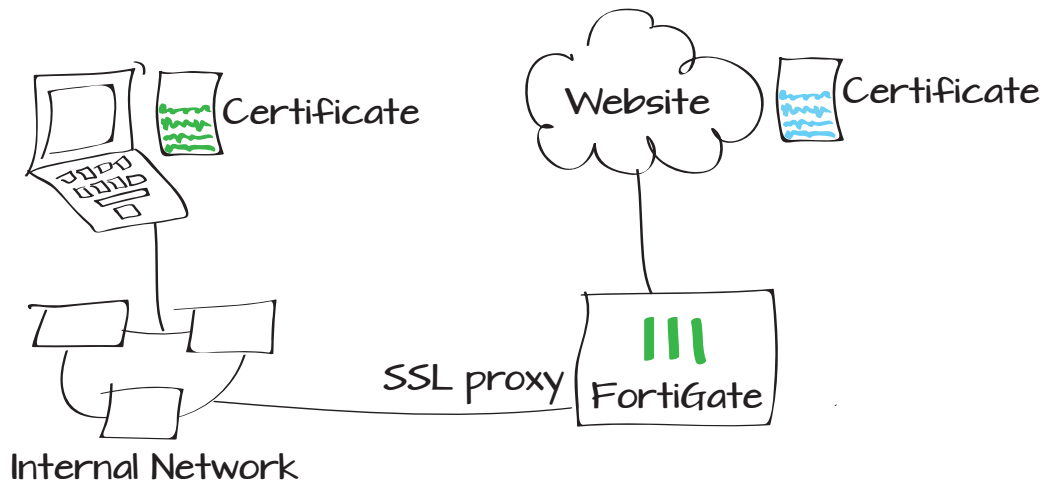




# Preventing security certificate warnings when using SSL inspection

This example illustrates how to prevent your users from getting a security certificate error, which happens because an SSL session is established with the SSL Proxy, not the destination website. Instead of having users select *Continue* when they receive an error, a bad habit to encourage, you will provide them with the FortiGate SSL CA certificate to install on their browsers.

1. Enabling Certificate configuration in the web-based manager.
2. Downloading the Fortinet\_CA\_SSLProxy.
3. Importing the CA certificate into the web browser.



## Enabling certificate configuration in the web-based manager

Go to **System > Config > Features** and enable **Certificates**.

## Downloading the Fortinet\_CA\_SSLProxy

Go to **System > Certificates > Local Certificates** to download the Fortinet\_CA\_SSLProxy certificate.

Make the CA certificate file available to your users.

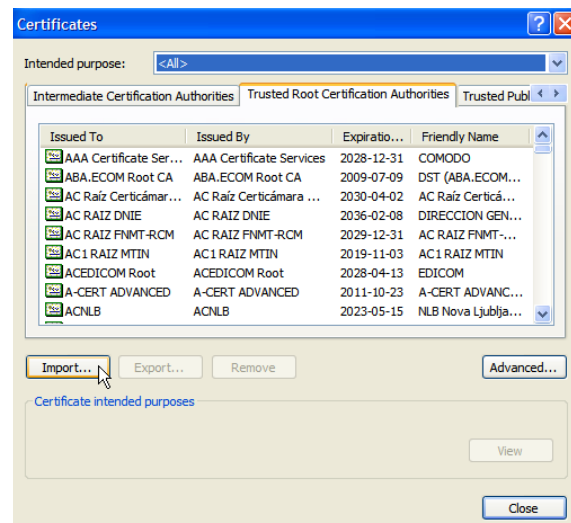
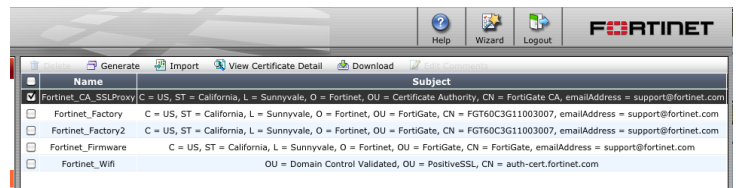
## Importing the CA certificate into the web browser

**For Internet Explorer:**

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

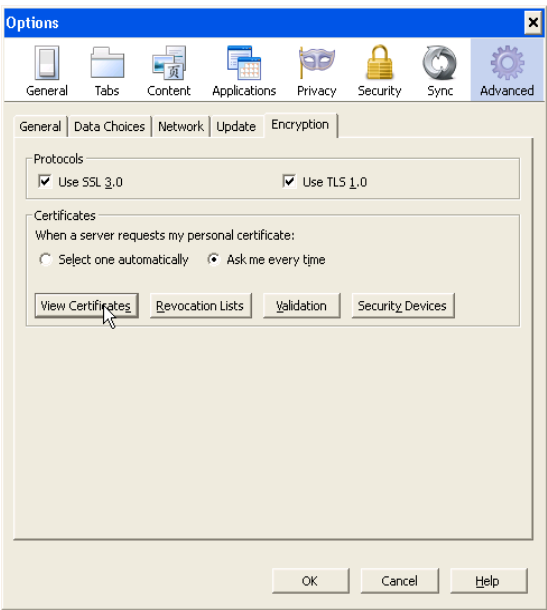
Import the certificate using the Import Wizard. Make sure that the certificate is imported into Trusted Root Certification Authorities.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select Yes to install the certificate.

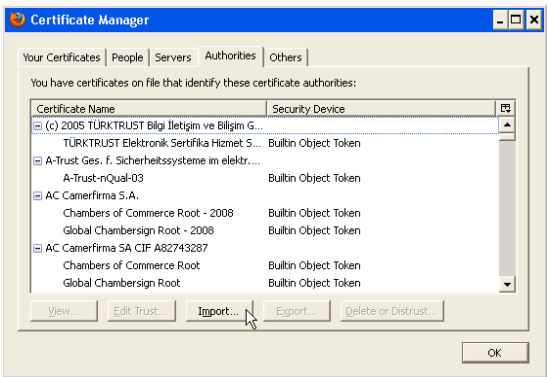


**For Firefox:**

Depending on platform, go to **Tools > Options** or **Edit > Preferences** and find the **Advanced Encryption** settings.



View Certificates, specifically the Authorities certificate list.

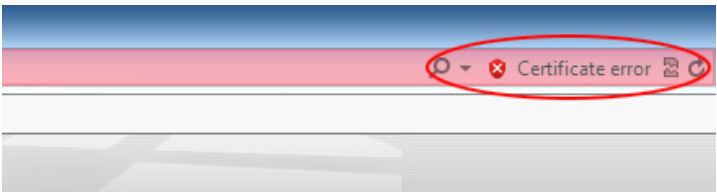


Import the Fortinet\_CA\_SSLProxy certificate file.

## Results

Even if you bypass the error message by selecting “Continue to this website”, the browser may still show an error in the toolbar.

After you install the FortiGate SSL CA certificate, there will be no certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.



## Extra help: Certificates

This section contains tips to help you with some common challenges of using certificates.

Certificate options do not appear in the GUI.

Go to **System > Features > Config** and select **Show More**. Enable the **Certificates** feature.

A new certificate must be used.

Go to **System > Certificates > Local Certificates** and select **Import**.

A new certificate must be generated.

First, go to **System > Certificates > Local Certificates** and select **Generate**. Fill in the required fields. The certificate must then be either self-signed or signed by a third party. Finally, import the new certificate.

Certificate warnings appear when users attempt to authenticate.

Go to **User & Device > Authentication > Settings** and set **Certificate** to use the correct certificate.

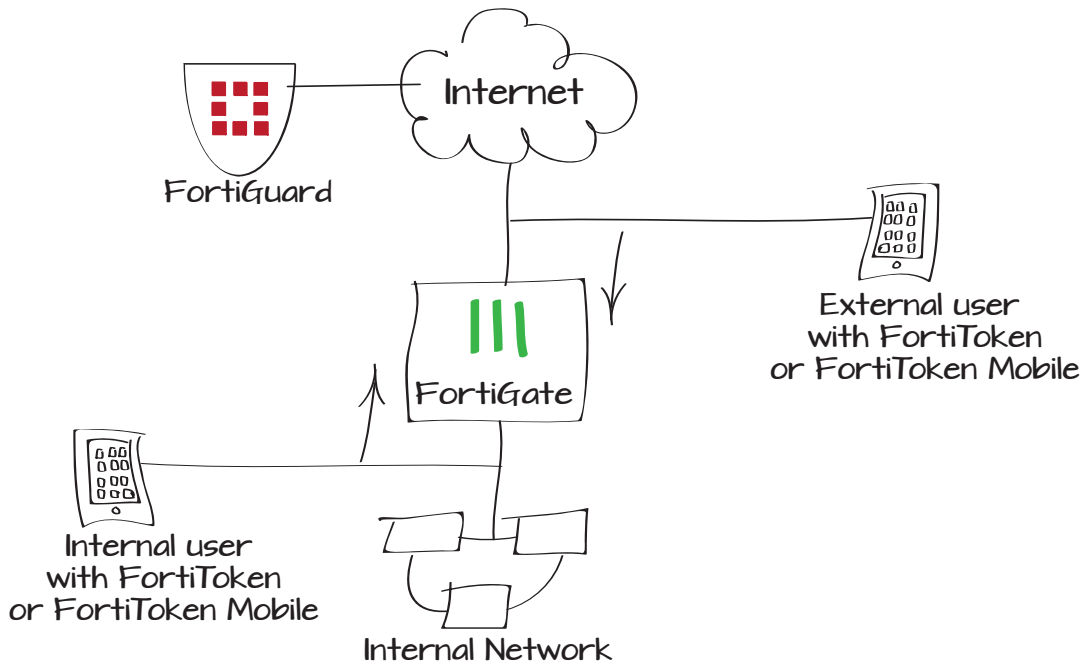
The wrong certificate appears when using an SSL-VPN.

Go to **VPN > SSL > Config** and set **Server Certificate** to use the correct certificate.

# Adding FortiToken two-factor authentication to a user account

Two-factor authentication enhances security because it requires both the user password - something that the user knows - and a dynamic token code provided by a FortiToken - something that the user has.

1. Registering FortiToken with a FortiGate unit and FortiGuard.
2. Adding two-factor authentication to the user's account.
3. Creating a policy that requires user authentication.



# Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.



If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.

Select **OK**.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate of one you have already entered.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.


Type

☒ Hard Token ☐ Mobile Token

Comments

0/255

Serial Number



Import

OK

Cancel

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	 Available		0	



# Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Enable Two-factor Authentication and select the FortiToken from the list. Select OK.

The following steps are only for confirmation.

The list of users (**User & Device > User > User Definition**) shows which users have two-factor authentication enabled.

The FortiTokens list (**User & Device > Two-factor Authentication > FortiTokens**) shows that the FortiToken is assigned to a user.

User Name

tbrown

☐ Disable

☒ Password

.....

☐ Match user on LDAP server

[Please Select]

☐ Match user on RADIUS server

[Please Select]

☐ Match user on TACACS+ server

[Please Select]

Contact Info

☐ Email Address

☒ SMS

☒ FortiGuard Messaging Service

☐ Custom

Phone Number

613-555-1200

☒ Enable Two-factor Authentication

Token

FTK2000BQL7PJW13

☒ Add this user to groups

☐ FortiGate\_Administrators

☐ SslvpnGroup

☐ WiFi\_users

☒ full-time

☐ part-time

OK

Cancel

User Name	Type	Two-factor Authentication	Ref.
blee	LOCAL	⊗	1
guest	LOCAL	⊗	0
jsmith	LOCAL	⊗	1
tbrown	LOCAL	FTK2000BQL7PJW13	1
telbar	LOCAL	⊗	2

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	<input checked="" type="checkbox"/> Assigned	tbrown	0	

## Creating a policy that requires user authentication

Go to **Policy > Policy > Policy** and create a User Identity policy with an authentication rule. This example allows the user tbrown to access the Internet (WAN1) from the Internal network (port1).



In this example we just add the user with the FortiToken to the policy. We could have added that user to a group and selected the user group.

## Results

When the user tries to access an Internet web site, the FortiGate unit requests user name and password authentication:

After successful ID/password authentication, the FortiGate requests the FortiToken code.

To obtain the token code:

- hard token: press the button on the FortiToken device
- soft token: use the FortiToken Mobile smartphone app to obtain the code

Incoming Interface	port1
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Group(s)	Click to add...
User(s)	tbrown
Schedule	always
Service	ALL
Action	ACCEPT

**FORTINET**  
**Authentication Required**

Please enter your username and password to continue.

Username: tbrown

Password: .....

Continue

**FORTINET**  
**FortiToken Code Required**

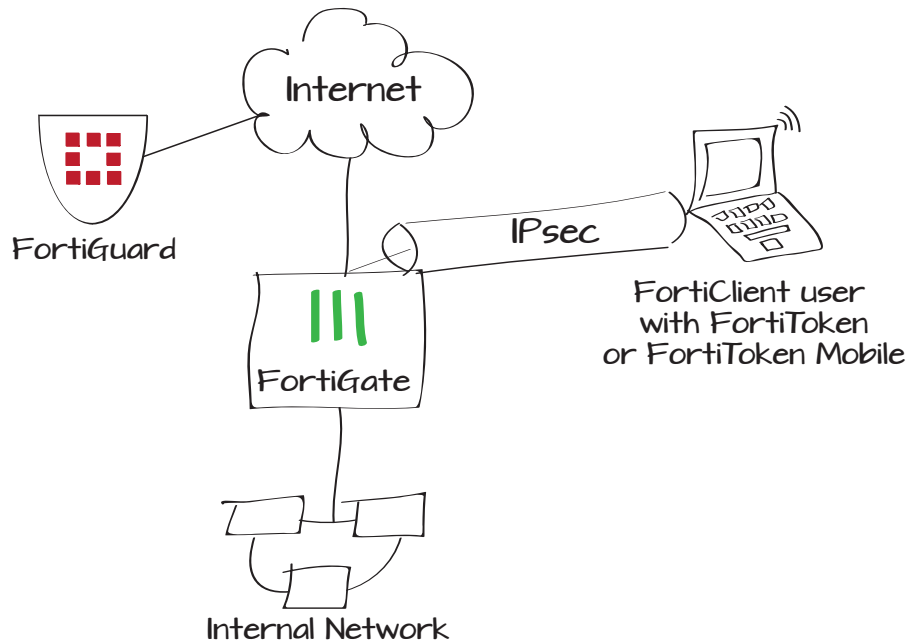
Token Code: 075159

Continue

# Using two-factor authentication with IPsec VPN

An IPsec VPN can use two-factor user authentication for enhanced security. In this example, a remote user uses FortiClient to connect to a private network behind a FortiGate unit. The FortiGate unit and FortiClient authenticate each other using a pre-shared key. The user is then authenticated by XAUTH (ID/password), plus a FortiToken token code.

1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the VPN on the FortiGate unit.
5. Configuring the VPN in FortiClient
6. Creating a security policy for VPN users



# Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number, its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Type

☒ Hard Token☐ Mobile Token

Comments

Write a comment...0/255

Serial Number

FTK2000BQL7PJW13

Import

OK

Cancel

Create NewEditDeleteRefresh

Search

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	Available		0	

## Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Enable Two-factor Authentication and select the FortiToken from the list. Select OK.

The screenshot shows the 'User Definition' configuration page for a user named 'tbrown'. The 'User Name' field is set to 'tbrown'. There are three radio buttons for authentication methods: 'Password' (selected), 'Match user on LDAP server', 'Match user on RADIUS server', and 'Match user on TACACS+ server'. Each of the latter three has a '[Please Select]' dropdown. Below this is the 'Contact Info' section with an 'Email Address' field and a checked 'SMS' option. The 'SMS' section has two radio buttons: 'FortiGuard Messaging Service' (selected) and 'Custom', with a 'Phone Number' field set to '613-555-1200'. The 'Enable Two-factor Authentication' section is checked, with a 'Token' dropdown set to 'FTK2000BQL7PJW13'. The 'Add this user to groups' section is checked, showing a list of groups: 'FortiGate\_Administrators', 'SslvpnGroup', 'WiFi\_users', 'full-time' (checked), and 'part-time'.

User Name: tbrown

☐ Disable

☒ Password

☐ Match user on LDAP server [Please Select]

☐ Match user on RADIUS server [Please Select]

☐ Match user on TACACS+ server [Please Select]

Contact Info

☐ Email Address

☒ SMS

☒ FortiGuard Messaging Service ☐ Custom

Phone Number: 613-555-1200

☒ Enable Two-factor Authentication

Token: FTK2000BQL7PJW13

☒ Add this user to groups

- ☐ FortiGate\_Administrators
- ☐ SslvpnGroup
- ☐ WiFi\_users
- ☒ full-time
- ☐ part-time

## Defining an address for the internal network

The VPN configuration and the firewall policy require a defined address for the Internal network.

Go to **Firewall Objects > Address > Addresses** and select **Create New**.

The screenshot shows the 'Address' configuration page for an address named 'Local LAN'. The 'Category' is set to 'Address' (selected). The 'Name' field is 'Local LAN'. The 'Color' field has a '[Change]' link. The 'Type' is set to 'Subnet'. The 'Subnet / IP Range' field is '192.168.1.0/255.255.255.0'. The 'Interface' is set to 'Any'. The 'Show in Address List' checkbox is checked. The 'Comments' field is 'Write a comment...' with a character count of 0/255.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name: Local LAN

Color: [Change]

Type: Subnet

Subnet / IP Range: 192.168.1.0/255.255.255.0

Interface: Any

Show in Address List: ☒

Comments: Write a comment... 0/255

## Configuring the VPN on the FortiGate unit

Go to **VPN > IPsec > Auto Key (IKE)** and select **Create VPN Wizard**.

Follow the wizard, entering the information that it requests.

The user group that you select determines who is allowed to connect to this VPN.

Clients will connect to the FortiGate unit through the WAN1 interface, which is connected to the Internet.

Address Range defines the IP address range to assign to clients.

Select the **Accessible Networks** for your clients, by selected the defined firewall address(es), or select All.

The options on the final wizard page can make the VPN more convenient to use. They are disabled by default.

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Name

VPN Type

☒ Dial Up - FortiClient Windows, Mac and Android

☐ Dial Up - iPhone / iPad Native IPsec Client

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Authentication Method ☒ Pre-shared Key ☐ RSA Signature

Pre-shared Key

User Group

1 VPN Setup 2 Authentication 3 Network 4 Client Options

Local Outgoing Interface

Address Range

Subnet Mask

DNS Server

☒ Use System DNS

☐ Specify

☒ Enable IPv4 Split Tunnel

Accessible Networks

☒ Allow Endpoint Registration

1 VPN Setup 2 Authentication 3 Network 4 Client Options

☐ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

# Creating a security policy for VPN users

Go to **Policy > Policy > Policy** and select **Create New**. Enter a policy to enable VPN users to authenticate and communicate with the local network.

Policy Type

☒ Firewall

☐ VPN

Policy Subtype

☐ Address

☒ User Identity

☐ Device Identity

Incoming Interface

fc\_vpn

Source Address

all

Outgoing Interface

port1

☒ Enable NAT

☒ Use Destination Interface Address

☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

☐ Use Central NAT Table

☐ Enable Web cache

☐ Enable WAN Optimization

Configure Authentication Rules

Create New

Edit

Delete

User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
full-time	Local LAN	ALL	always	-			ACCEPT
ANY	all	ALL	always	-			DENY

☐ Skip this policy for unauthenticated user

☐ Disclaimer

☐ Customize Authentication Messages

Tags

Applied tags

Add tag

Comments

Write a comment...

0/1023

OK

Cancel

## Configuring the VPN in FortiClient

In the FortiClient Console, select **Remote Access**, then select **Configure VPN**.



If FortiClient has other VPNs configured, select **Add a new connection** from the menu.

Enter the VPN configuration and select OK.

The screenshot shows the FortiClient interface with a dropdown menu open for the 'VPN1' connection. The menu options are: 'Add a new connection' (highlighted with a mouse cursor), 'Edit the selected connection', and 'Delete the selected connection'. Below the menu, there are input fields for 'Username' and 'Password'.

The screenshot shows the 'Configure VPN' form in FortiClient. The fields are: 'Connection Name' (Office), 'Type' (SSL-VPN and IPsec VPN, with IPsec VPN selected), 'Description' (empty), 'Remote Gateway' (172.20.120.123), 'Authentication Method' (Pre-Shared Key), 'Pre-Shared Key' (masked with dots), and 'Authentication (XAuth)' (Prompt on login and Save login, with Prompt on login selected).



# Results

In FortiClient console, select Remote Access. Select the VPN and enter the user name and password.

After connecting and authenticating by user name and password, FortiClient requests the FortiToken code.


Get the code from the FortiToken (hard token), or FortiToken Mobile app (soft token) and enter it.

If the token code is correct, the VPN connects and FortiClient minimizes its window.

On the FortiGate unit, the **VPN > Monitor > IPsec Monitor** page shows the connected client.

 Office





tbrown



•••••

☐ Auto Connect

Connect



245542

FortiToken Code

☐ Auto Connect

OK

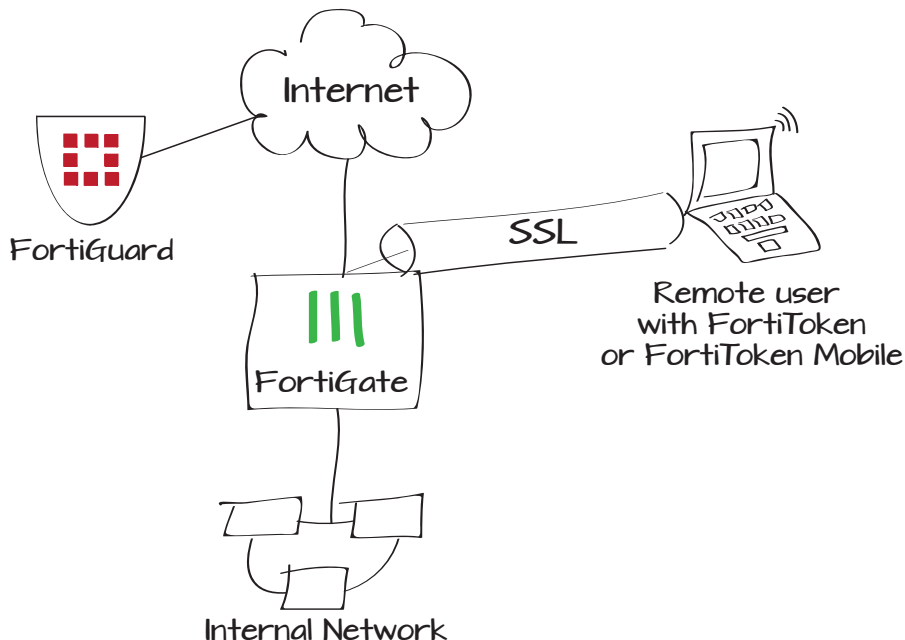
Cancel

Name	Type	Username	Remote Gateway	Proxy ID	Destination
fc_vpn_0	Dialup	tbrown	172.20.120.52	10.11.10.1-10.11.10.1	

# Using two-factor authentication with SSL VPN

An SSL VPN can use two-factor user authentication for enhanced security. In this example, a remote user uses FortiClient to connect to a private network behind a FortiGate unit. The FortiGate unit and FortiClient authenticate each other using a pre-shared key. The user is authenticated by User ID/password) plus a FortiToken token code.

1. Registering FortiToken with a FortiGate unit and FortiGuard
2. Adding two-factor authentication to the user's account
3. Defining an address for the internal network
4. Configuring the SSL VPN on the FortiGate unit.
5. Creating a security policy for SSL VPN users



# Registering FortiToken with a FortiGate unit and FortiGuard

Go to **User & Device > Two-factor Authentication > FortiTokens** and select **Create New**. Select the **Serial Number** field and enter the FortiToken serial number.

If you have several FortiTokens to add, you can list their serial numbers one per line in a text file and use the Import function.



FortiOS reports the serial number as invalid if you mistype it or if it is a duplicate.

Wait for the FortiGuard to validate your FortiToken's serial number. When you first enter the serial number its status is listed as **Pending**. When FortiGuard validates the serial number, the status changes to **Available**.



If this FortiToken has already been registered to another FortiGate unit, the Status column shows Error.

Type

☒ Hard Token ☐ Mobile Token

Comments

0/255

Serial Number

Import

OK

Cancel

Type	Serial Number	Status	User	Drift	Comments
	FTK2000BQL7PJW13	Available		0	

## Adding two-factor authentication to the user's account

Go to **User & Device > User > User Definition** and open the user's account for editing.

Select **Enable Two-factor Authentication** and then select the FortiToken from the list. Select OK.

The screenshot shows the 'User Definition' configuration page for a user named 'tbrown'. The 'Password' section is active, showing a masked password and options to match users on LDAP, RADIUS, or TACACS+ servers. The 'Contact Info' section has 'Email Address' disabled and 'SMS' enabled, with a 'FortiGuard Messaging Service' selected and a phone number of '613-555-1200'. The 'Enable Two-factor Authentication' section is checked, with a token 'FTK2000BQL7PJW13' selected. A list of groups is shown, with 'full-time' selected. At the bottom are 'OK' and 'Cancel' buttons.

User Name: tbrown

☐ Disable

☒ Password: \*\*\*\*\*

☐ Match user on LDAP server: [Please Select]

☐ Match user on RADIUS server: [Please Select]

☐ Match user on TACACS+ server: [Please Select]

Contact Info

☐ Email Address

☒ SMS: ☒ FortiGuard Messaging Service ☐ Custom

Phone Number: 613-555-1200

☒ Enable Two-factor Authentication

Token: FTK2000BQL7PJW13

☒ Add this user to groups

- ☐ FortiGate\_Administrators
- ☐ SslvpnGroup
- ☐ WiFi\_users
- ☒ full-time
- ☐ part-time

OK Cancel

## Defining an address for the internal network

Go to **Firewall Objects > Address > Addresses** and select **Create New**.

The VPN configuration and the firewall policy require a defined address for the Internal network.

The screenshot shows the 'Address' configuration page for a new address named 'Local LAN'. The 'Category' is set to 'Address'. The 'Type' is 'Subnet'. The 'Subnet / IP Range' is '192.168.1.0/255.255.255.0'. The 'Interface' is 'Any'. The 'Show in Address List' checkbox is checked. The 'Comments' field is empty. At the bottom are 'OK' and 'Cancel' buttons.

Category: ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name: Local LAN

Color: [Change]

Type: Subnet

Subnet / IP Range: 192.168.1.0/255.255.255.0

Interface: Any

Show in Address List: ☒

Comments: Write a comment... 0/255

OK Cancel







## Creating a user group for SSL VPN users

Go to **User & Device > User > User Groups** and create a Firewall type user group, adding the users who will be permitted to use the SSL VPN.

## Configuring an SSL VPN web portal

Go to **VPN > SSL > Config**.

The default encryption will work with typical browsers.

Name	<input type="text" value="full-time"/>
Type	<input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest
Members	<div><div> tbrown <span>✕</span></div><div> jsmith <span>✕</span></div><div> blee <span>✕</span></div></div> <div></div>
<hr/>	
IP Pools	<input type="text" value="SSLVPN_TUNNEL_ADDR1"/> <span>✕</span> 
<hr/>	
Server Certificate	<input type="text" value="Self-Signed"/>
Require Client Certificate	<input type="checkbox"/>
Encryption Key Algorithm	<input type="radio"/> High - AES(128/256 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) and higher <input type="radio"/> Low - RC4(64 bits), DES and higher
Idle Timeout	<input type="text" value="300"/> (seconds)
Login Port	<input type="text" value="10443"/>
<input type="checkbox"/> Allow Endpoint Registration (Tunnel Mode Only)	
<hr/>	
 <b>Advanced</b> (DNS and WINS Servers)	
<div><div>Apply</div></div>	

Go to **VPN > SSL > Portal**.

Creating a security policy for SSL VPN users

Go to **Policy > Policy > Policy** and select **Create New**. Enter a policy to enable VPN users to authenticate and communicate with the local network.

Name:web-access

Portal Message:Welcome to SSL VPN Service

Theme:Blue

Page Layout:

☐ Enable Tunnel Mode

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS

☒ SSH

☒ CITRIX

☒ FTP

☒ TELNET

☒ RDP NATIVE

☒ RDP

☒ VNC

☒ Port Forward

☒ SMB/CIFS

☐ PING

☒ Include Session Info

☐ Include Connection Tool

☐ Include FortiClient Download

☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
No matching entries found			

☒ Prompt Mobile Users to Download FortiClient App

☒ Allow Multiple Concurrent Sessions For Each User

View Portal

Apply

Policy Type

☐ Firewall

☒ VPN

Policy Subtype

☐ IPsec

☒ SSL-VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1

Local Protected Subnet

Local LAN

☐ SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create NewEditDelete

User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
<div><div>full-time</div></div>	ALL	always	-	full-access	<div><div></div></div>	<div><div>ACCEPT</div></div>
<div><div>ANY</div></div>	ALL	always	-		-	<div><div>DENY</div></div>

Tags

Applied tags

Add tag

Comments

Write a comment...

0/1023

OK

Cancel

310

The FortiGate Cookbook 5.0.7

# Results

In a browser, enter the FortiGate IP address and port 10443. For example https://172.20.120.123:10443.

If you receive a warning about the certificate being unrecognized, allow the browser to continue access.

Enter the user name and password and then select **Login**. If the user account has two-factor authentication enabled, the **FortiToken Code** field is added. Obtain the code from the FortiToken device or FortiToken Mobile app and enter it. Select **Login** again.

You are connected to the SSL VPN portal.

The **VPN > Monitor > SSL-VPN Monitor** page shows the connected SSL VPN client.

Please Login

Name:

tbrown

Password:

.....

FortiToken Code:

.....

Login

Welcome to SSL VPN Service

Session Information

Time Logged In:

tbrown (0 hour(s), 0 minute(s), 41 second(s))

HTTP Inbound/Outbound Traffic:

0 bytes / 0 bytes

HTTPS Inbound/Outbound Traffic:

0 bytes / 0 bytes

Remote Desktop

Windows server

telbar PC

Add

Edit

Tunnel Mode

Connect

Disconnect

Refresh

Link status:

Bytes sent:

Bytes received:

Collecting information...

Connection Tool

Type:

HTTP/HTTPS

Host:

Go

	No.	User	Source IP	Begin Time	Description
<input type="checkbox"/>	1	tbrown	172.20.120.52	Thu Sep 12 10:04:32 2013	
<input type="checkbox"/>			Subsession		Tunnel IP:10.212.134.200

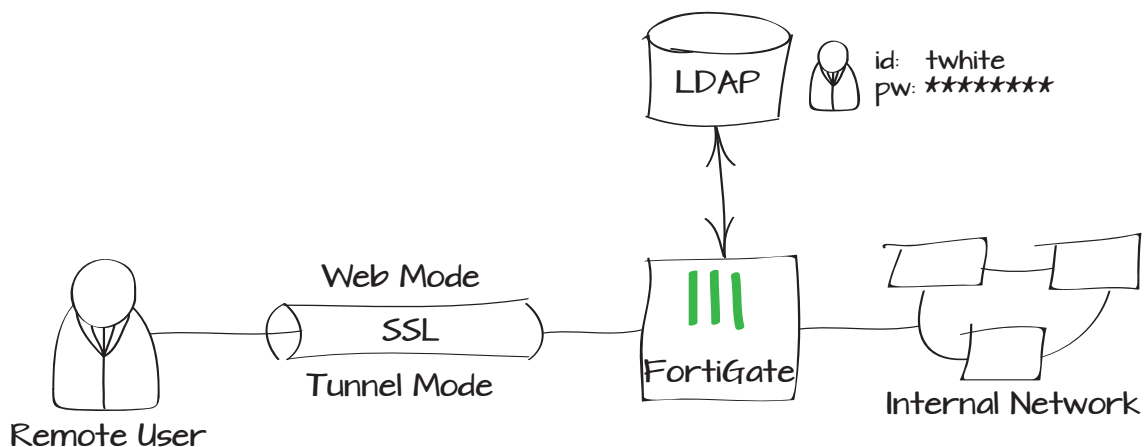
# Authenticating SSL VPN users using LDAP

This example illustrates how to configure a FortiGate to use LDAP authentication to authenticate remote SSL VPN users. With a properly configured LDAP server, user and authentication data can be maintained independently of the FortiGate, accessed only when a remote user attempts to connect through the SSL VPN tunnel.



This recipe assumes that the LDAP server is already configured.

1. Registering the LDAP server on the FortiGate
2. Importing LDAP users
3. Creating the SSL VPN user group
4. Creating the SSL address range
5. Configuring the SSL VPN tunnel
6. Creating security policies
7. Results





## Registering the LDAP server on the FortiGate

Go to **User & Device > Authentication > LDAP Servers** and select **Create New**.

Enter the LDAP Server's FQDN or IP in **Server Name/IP**. If necessary, change the Server Port Number (the default is 389.)

Enter the **Common Name Identifier**. Most LDAP servers use "cn" by default.

In the **Distinguished Name** field, enter the base distinguished name for the server, using the correct X.500 or LDAP format.

Set the **Bind Type** to **Regular**, and enter the LDAP administrator's distinguished name and password for **User DN** and **Password**.

Name	<input type="text" value="Example_LDAP"/>
Server Name/IP	<input type="text" value="10.10.10.1"/>
Server Port	<input type="text" value="389"/>
Common Name Identifier	<input type="text" value="cn"/>
Distinguished Name	<input type="text" value="Example LDAP Server"/>
Bind Type	<input type="radio"/> Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
User DN	<input type="text" value="example_admin"/>
Password	<input type="password" value="....."/>
<input type="checkbox"/> Secure Connection	

## Importing LDAP users

Go to **User & Device > User > User Definition**, and create a new user, selecting **Remote LDAP User**.

Choose your LDAP Server from the dropdown list.

You will be presented with a list of user accounts, filtered by the LDAP Filter to include only common user classes.



If you are using a different objectClass to identify users on your LDAP server, edit the filter to show them in the list.

### 1 Choose User Type > 2 Specify LDAP Server

- ☐ Local User
- ☐ Remote RADIUS User
- ☐ Remote TACACS+ User
- ☒ Remote LDAP User

### 1 Choose User Type > 2 Specify LDAP Server > 3 Select Remote Users

- ☒ Choose Existing
- ☐ Create New

Select the users you want to register as users on the FortiGate, and select **Next**.

Confirm that the user information has been imported properly, and select **Done**.

## Creating the SSL VPN user group

Go to **User & Device > User > User Groups**, and create an LDAP user group.

Add all of the user accounts imported from LDAP to the **Members** list.



If you have already configured user groups on the LDAP server, you can use the **Remote Groups** menu to import them.

## Creating the SSL address ranges

Go to **Firewall Objects > Addresses > Addresses**, and create a new address.

Set the **Type** to **IP Range**, and in the **Subnet/IP Range** field, enter the range of addresses you want to assign to SSL VPN clients. Select **Any** as the **Interface**.

Then create another Address for each Subnet or IP Range within your internal network to which remote users will connect.

Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐

Members

Remote groups

Remote Server
Example_LDAP

Category ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Category ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

# Configuring the SSL VPN tunnel

Go to **VPN > SSL > Portal**, and select the plus icon in the upper right to create a new SSL Portal configuration.

Enable **Tunnel Mode**, and enable **Split Tunneling**. For the **IP Pool**, select the address range you created. Enable **Web Mode**, and set the options as desired.

Enable **Include Bookmarks**, and create a bookmark to access a internal network PC. In this example, the bookmark is an **RDP** connection, for remote desktop access.



By default, SSL authentication expires after 28800 seconds (8 hours). This limit can be changed in the CLI:  
`config vpn ssl settings`  
`set auth-timeout`

# Creating security policies

You will need to create two policies to handle web mode and tunnel mode SSL traffic.

Go to **Policy > Policy > Policy**, and create a new **VPN** policy to allow the SSL traffic through to the internal network.

Set the **Incoming Interface** to your Internet-facing interface, your **Remote Address** to all, your **Local Interface** to your internal network interface, and for the **Local Protected Subnet**, select the network access addresses you created.

Name:LDAP\_full\_access

Portal Message:Welcome to SSL VPN Service

Theme:SteelBlue

Page Layout:

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

IP Pools

LDAP\_SSL\_range

Client Options

☐ Save Password

☐ Auto Connect

☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS

☒ SSH

☒ CITRIX

☒ FTP

☒ TELNET

☒ RDP NATIVE

☒ RDP

☒ VNC

☐ Port Forward

☒ SMB/CIFS

☒ PING

☒ Include Session Info

☐ Include Connection Tool

☒ Include FortiClient Download

☐ Include Login History

☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
RDP (1)			
RDP_example	RDP	192.168.1.144	

☒ Prompt Mobile Users to Download FortiClient App

☒ Allow Multiple Concurrent Sessions For Each User

Policy Type

☐ Firewall

☒ VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1 (Internal)

Local Protected Subnet

Local Network Subnet

Under **Configure SSL-VPN Authentication Rules**, select **Create New** to create a new rule to govern SSL traffic.

Set the **Group** to your SSL VPN group, select your LDAP user as **User**, and select your **SSL-VPN Portal** from the list.

Configure the logging and security profiles as needed.

Return to the policy list, and select **Create New** again, to create the tunnel mode firewall policy. Leave the **Type** as **Firewall**, and the **Subtype** as **Address**.

Set the **Incoming Interface** to the SSL VPN tunnel interface. Set the **Source Address** to the VPN users address range. Set the **Outgoing Interface** to the internal network interface, and set the **Destination Address** to the internal network addresses that SSL users will need to reach.

Enable **NAT**, and configure logging and security policies as needed.

Group(s)

SSLVPN\_LDAP\_group

User(s)

twhite

Schedule

always

SSL-VPN Portal

LDAP\_SSL Portal

Action

ACCEPT

Logging Options

No Log

Log Security Events

Log all Sessions

Security Profiles

ON

 AntiVirus

OFF

 Web Filter

ON

 Application Control

OFF

 IPS

OFF

 Email Filter

ON

 DLP Sensor

OFF

 VoIP

OFF

 ICAP

default

default

default

default

default

default

default

Policy Type

Firewall VPN

Policy Subtype

Address User Identity Device Identity

Incoming Interface

ssl.root (sslvpn tunnel interface)

Source Address

LDAP\_SSL\_range

Outgoing Interface

port1 (Internal)

Destination Address

Local Network Subnet

Schedule

always

Service

ALL

Action

ACCEPT

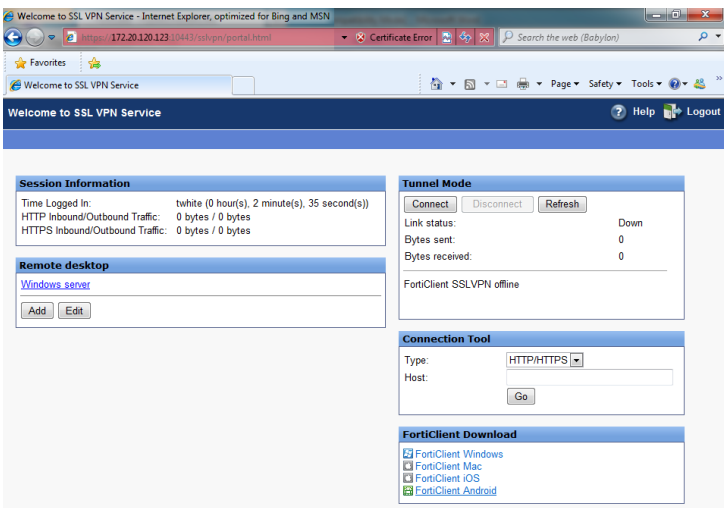
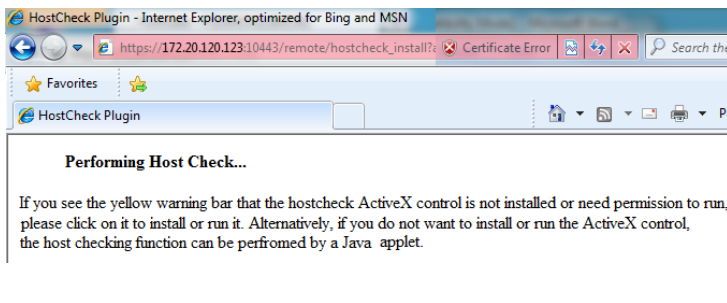
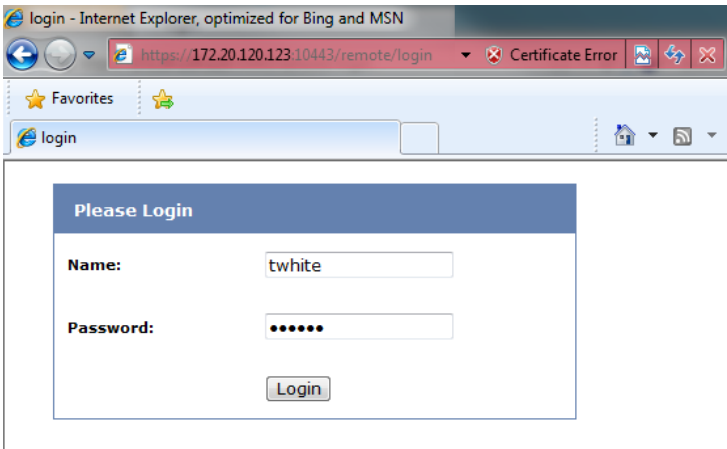
Enable NAT

# Results

Log into the SSL portal using the LDAP user credentials. The FortiGate will automatically contact the LDAP server for verification.

The FortiGate unit performs the host check.

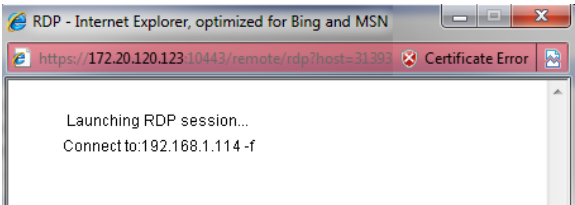
After the check is complete, the SSL portal appears.



Select a bookmark, such as the **RDP** link, to begin an RDP session, and connect to a PC on the internal network.

Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

Go to **Log & Report > Traffic Log > Forward Traffic** to see details about SSL traffic.



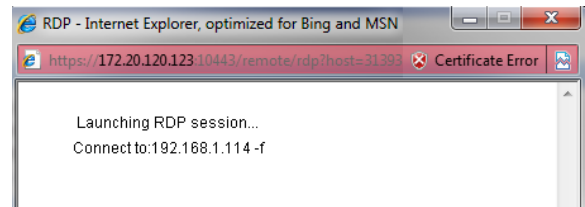
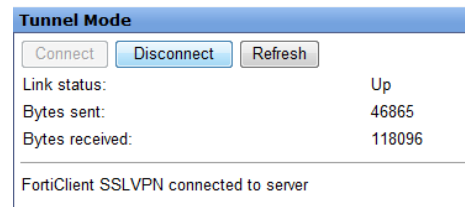
No.	User	Source IP	Begin Time	Desc
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Web Application:RDP 192.168.1.114		

Dst	192.168.1.114	Virtual Domain	root
Received	85591	Source Country	Reserved
Sent / Received	8.71 KB / 83.58 KB	Duration	36
Sent	8923	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	✓
Timestamp	Wed Apr 17 14:13:11 2013	Tran Display	noop
Sequence Number	2700	Policy ID	11
Src Interface	wan1	Src	twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	71
Level	notice	VPN Type	sslvpn
Src Port	53712	Log ID	13
Sub Type	forward	Threat	
Received Packets	98	Date/Time	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.

Select the **RDP** bookmark to begin an RDP session.

Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Tunnel description indicates that the user is using tunnel mode.



User	Source IP	Begin Time	Descrip
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession			Tunnel IP:10.212.134.200

# SSL and IPsec VPN

Virtual private networks (VPNs) extend a private network across a public network, typically the Internet. Two types of VPN can be configured with FortiGate unit: SSL VPN and IPsec VPN.

SSL VPN configuration requires an SSL VPN web portal for users to log into, a user authentication configuration for SSL VPN users, and the creation of SSL VPN security policies that control the source and destination access of SSL VPN users.

IPsec supports a similar client server architecture as SSL VPN. However, to support a client server architecture, IPsec users must install and configure an IPsec VPN client (such as FortiClient) on their PCs or mobile devices.

This section contains the following examples:

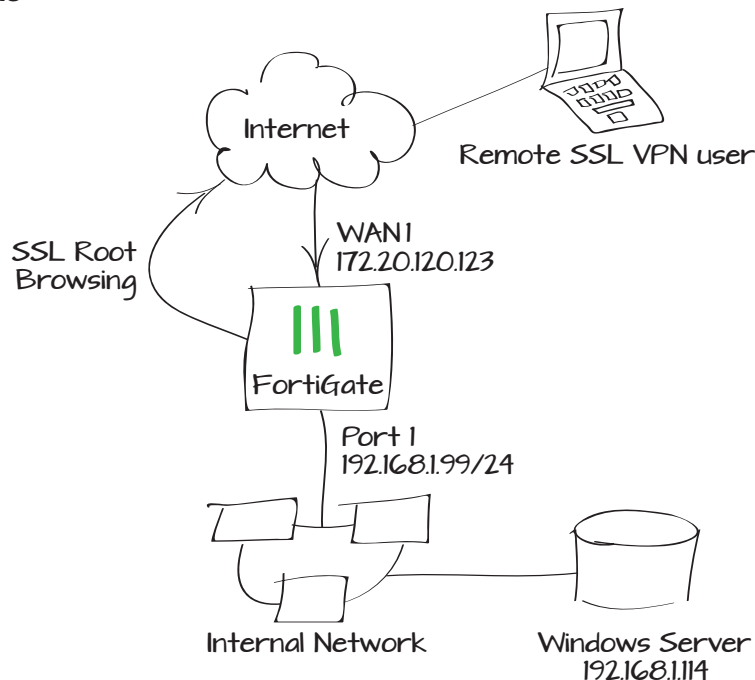
- [Providing remote users with access using SSL VPN](#)
- [Connecting an Android to a FortiGate with SSL VPN](#)
- [Configuring SSL VPN with strong authentication using certificates](#)
- [Using IPsec VPN to provide communication between offices](#)
- [Extra help: IPsec VPN](#)
- [Using policy-based IPsec VPN for communication between offices](#)
- [Providing secure remote access to a network for an iOS device](#)
- [Connecting an Android to a FortiGate with IPsec VPN](#)
- [Configuring a FortiGate unit as an L2TP/IPsec server](#)
- [Configuring IPsec VPN with a FortiGate and a Cisco ASA](#)
- [Creating a VPN with overlapping subnets](#)
- [Using redundant OSPF routing over IPsec VPN](#)



# Providing remote users with access using SSL VPN

This example provides remote users with access to the corporate network using SSL VPN and connection to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Adding security policies for access to the Internet and internal network
5. Setting the FortiGate unit to verify users have current antivirus software
6. Results



# Creating an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portal**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

Select **Create New** in the **Include Bookmarks** area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

Name:full-access

Portal Message:Welcome to SSL VPN Service

Theme:Blue

Page Layout:

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

IP Pools

SSLVPN\_TUNNEL\_ADDR1

Client Options

☐ Save Password☐ Auto Connect☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS☒ SSH☒ CITRIX

☒ FTP☒ TELNET☒ RDP NATIVE

☒ RDP☒ VNC☒ Port Forward

☒ SMB/CIFS☒ PING

☒ Include Session Info☒ Include Connection Tool☒ Include FortiClient Download☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
No matching entries found			

☒ Prompt Mobile Users to Download FortiClient App☒ Allow Multiple Concurrent Sessions For Each User

View Portal

CategoryRemote desktop

NameWindows server

TypeRDP

Location192.168.1.114

Screen Width1024

Screen Height768

Logon User

Logon Password

Keyboard LayoutEnglish, US

Description

Full Screen Mode☒

## Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, 'twhite').

Go to **User & Device > User > User Groups**.

Add the user to a user group for SSL VPN connections.

The image displays four sequential screenshots of the FortiGate User Creation Wizard, illustrating the process of creating a remote user and adding them to a user group.

**Screenshot 1: Choose User Type**  
Step 1 of 4. Options: ☒ Local User, ☐ Remote RADIUS User, ☐ Remote TACACS+ User, ☐ Remote LDAP User. Buttons: < Back, Next >, Cancel.

**Screenshot 2: Specify Login Credential**  
Step 2 of 4. Fields: User Name (twhite), Password (masked). Buttons: < Back, Next >, Cancel.

**Screenshot 3: Provide Contact Info**  
Step 3 of 4. Fields: Email Address (twhite@example.com), SMS (checked), Phone Number (55555555), Service Type (FortiGuard Messaging Service). Buttons: < Back, Next >, Cancel.

**Screenshot 4: Provide Extra Info**  
Step 4 of 4. Options: ☒ Enable, ☐ Two-factor Authentication, ☐ User Group. Buttons: < Back, Done, Cancel.

**User Group Configuration**  
Name: sslvpn\_group  
Type: ☒ Firewall, ☐ Fortinet Single Sign-On (FSSO), ☐ Guest, ☐ RADIUS Single Sign-On (RSSO)  
Available Users: - Local Users - guest  
Members: - Local Users - twhite

# Adding an address for the local network

Go to **Firewall Objects > Address > Addresses**.

Add the address for the local network. Set **Type** to **Subnet**, **Subnet/ IP Range** to the local subnet, and **Interface** to an internal port.

# Adding security policies for access to the Internet and internal network

Go to **Policy > Policy > Policy**.

Add a security policy allowing access to the internal network. Set **Type** to **VPN** and **Subtype** to **SSL-VPN**.



If your FortiGate unit does not have the Policy-based IPsec feature turned on, you will only have to set **Policy Type** to **VPN**.

Set **Incoming Interface** to your Internet-facing interface, **Local Interface** to an internal port and **Local Protected Subnet** to the address for the local network. Create a new **Authentication Rule** to allow the remote user group access.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Show in Address List

☒

Comments

Write a comment... 0/255

Policy Type

☐ Firewall ☒ VPN

Policy Subtype

☐ IPsec ☒ SSL-VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1

Local Protected Subnet

Local LAN

☐ SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create New	Edit	Delete				
User/Group	Service	Schedule	UTM Security	SSL-VPN Portal	Logging	Action
sslvpn_group	ALL	always	-	full-access		ACCEPT
ANY	ALL	always	-			DENY

Tags

Applied tags

Add tag

Comments

Write a comment... 0/1023

Add a second security policy allowing access to the Internet.

For this policy, **Incoming Interface** is *sslvpn tunnel interface* and **Outgoing Interface** is your Internet-facing interface.

## Setting the FortiGate unit to verify users have current antivirus software

Go to **System > Status > Dashboard**.

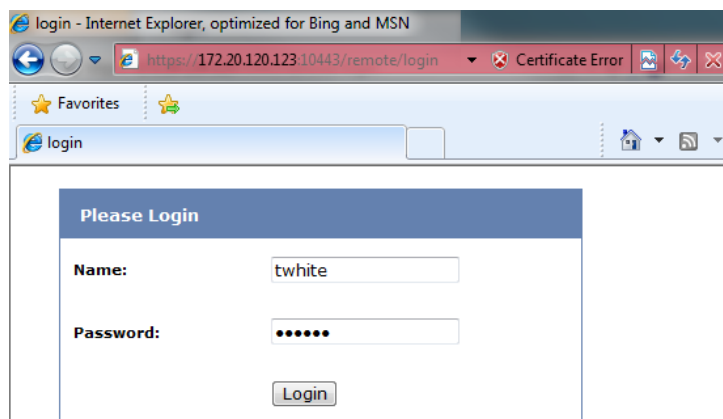
In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant antivirus software on the remote user's computer.

## Results

Log into the portal using the credentials you created in step two.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	sslvpn tunnel interface
Source Address	SSLVPN_TUNNEL_ADDR1
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	

```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
#
```

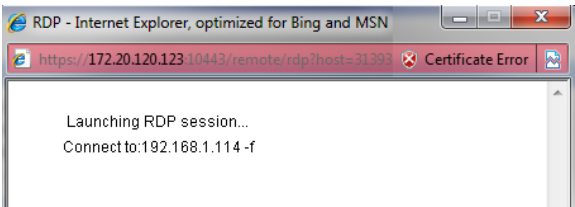
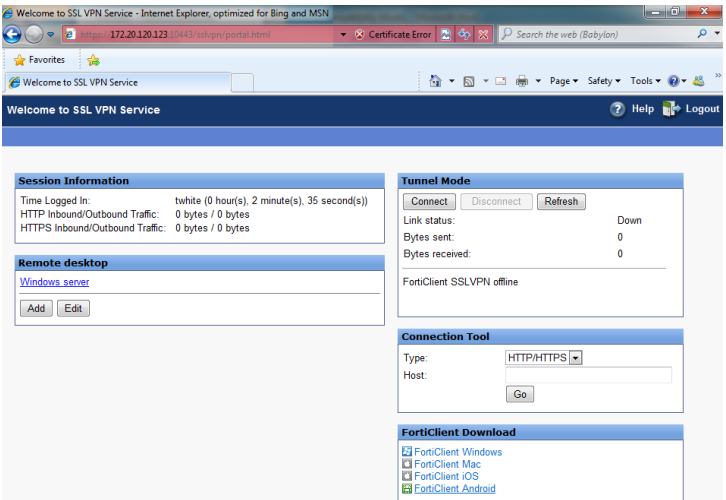
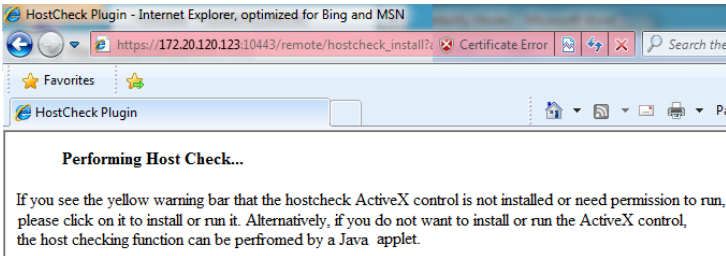


The FortiGate unit performs the host check.

After the check is complete, the portal appears.





Select the bookmark **Remote Desktop** link to begin an RDP session.

Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.



No.	User	Source IP	Begin Time	Desc
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Web Application:RDP 192.168.1.114		

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	Virtual Domain	root
Received	85591	Source Country	Reserved
Sent / Received	8.71 KB / 83.58 KB	Duration	36
Sent	8923	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	
Timestamp	Wed Apr 17 14:13:11 2013	Tran Display	noop
Sequence Number	2700	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	71
Level	notice 	VPN Type	sslvpn
Src Port	53712	Log ID	13
Sub Type	forward	Threat	
Received Packets	98	Date/Time	14:13:11 (Wed Apr 17 14:
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.

Tunnel Mode

Connect

Disconnect

Refresh

Link status:

Up

Bytes sent:

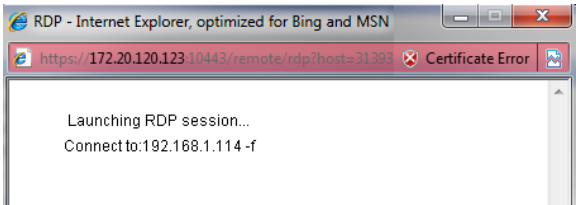
46865

Bytes received:

118096

FortiClient SSLVPN connected to server

Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.





User	Source IP	Begin Time	Descri
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Tunnel IP:10.212.134.200	








Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.



Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

Select an entry to view more information.

Dst	192.168.1.114	Virtual Domain	root
Received	326664	Source Country	Reserved
Sent / Received	54.36 KB / 319.01 KB	Duration	83
Sent	55665	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	
Timestamp	Wed Apr 17 14:17:15 2013	Tran Display	noop
Sequence Number	3618	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	329
Level	notice 	VPN Type	sslvpn
Src Port	53820	Log ID	13
Sub Type	forward	Threat	
Received Packets	407	Date/Time	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

Refresh  Download Raw Log					
#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst
▶ 1	14:26:05	ssl.root	wan1	10.212.134.200	 74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	 66.171.121.34 (fortinet.c
5	14:25:57	ssl.root	wan1	10.212.134.200	 74.121.50.17 (www.page
6	14:25:44	ssl.root	wan1	10.212.134.200	 208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30

Dst	 66.171.121.34 (fortinet.com)	Virtual Domain	root
Received	938	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	535 B / 938 B
Duration	17	Sent	535
Src NAT Port	54165	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65389	Status	close
Timestamp	Wed Apr 17 14:26:03 2013	Tran Display	snat
Sequence Number	8096	Policy ID	8
Src Interface	ssl.root	Src	10.212.134.200
Sent Packets	6	Level	notice 
Src Port	54165	Log ID	13
Sub Type	forward	Threat	
Received Packets	5	Date/Time	14:26:03 (Wed Apr 17 14:26:03 2013)
Dst Interface	wan1		



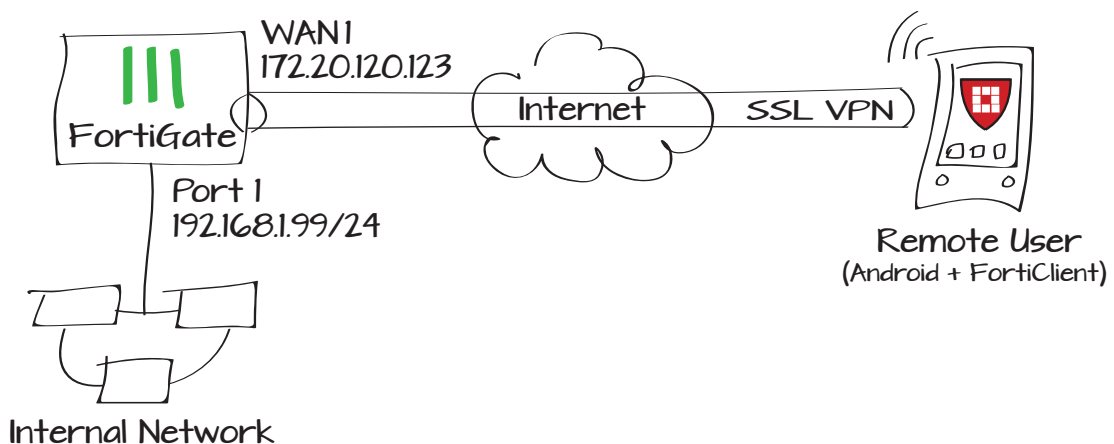
# Connecting an Android to a FortiGate with SSL VPN

This recipe describes how to provide a group of remote Android users with secure, encrypted access to the network using FortiClient and SSL VPN.



You must download the FortiClient application from the Play Store and install it on your Android device. Refer to the [FortiClient for Android QuickStart Guide](#). This recipe was tested using Android version 4.3.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the network
4. Adding security policies for access to the Internet and internal network
5. Configuring the tunnel on FortiClient for Android
6. Results



# Creating an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portal**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

Select **Create New** in the **Include Bookmarks** area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

Name:full-access

Portal Message:Welcome to SSL VPN Service

Theme:Blue

Page Layout:

☒ Enable Tunnel Mode

☐ Enable Split Tunneling

IP Pools

SSLVPN\_TUNNEL\_ADDR1

Client Options

☐ Save Password☐ Auto Connect☐ Always Up (Keep Alive)

☒ Enable Web Mode

Applications

☒ HTTP/HTTPS☒ SSH☒ CITRIX

☒ FTP☒ TELNET☒ RDP NATIVE

☒ RDP☒ VNC☒ Port Forward

☒ SMB/CIFS☒ PING

☒ Include Session Info☒ Include Connection Tool☒ Include FortiClient Download☒ Include Bookmarks

Create NewEdit SSL-VPN PortalDelete

Name	Type	Location	Description
No matching entries found			

☒ Prompt Mobile Users to Download FortiClient App☒ Allow Multiple Concurrent Sessions For Each User

View Portal

CategoryRemote desktop

NameWindows server

TypeRDP

Location192.168.1.114

Screen Width1024

Screen Height768

Logon User

Logon Password

Keyboard LayoutEnglish, US

Description

Full Screen Mode☒

## Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, 'twhite').

Go to **User & Device > User > User Groups**.

Add the user to a user group for SSL VPN connections.

The image displays four sequential screenshots of the FortiGate User Creation Wizard, illustrating the steps to create a remote user and add them to a user group.

**Screenshot 1: Step 1 - Choose User Type**

- Progress bar: 1 Choose User Type, 2 Specify Login Credential, 3 Provide Contact Info, 4 Provide Extra Info
- Options:
  - ☒ Local User
  - ☐ Remote RADIUS User
  - ☐ Remote TACACS+ User
  - ☐ Remote LDAP User
- Buttons: < Back, Next >, Cancel

**Screenshot 2: Step 2 - Specify Login Credential**

- Progress bar: 1 Choose User Type, 2 Specify Login Credential, 3 Provide Contact Info, 4 Provide Extra Info
- Fields:
  - User Name: twhite
  - Password: [masked]
- Buttons: < Back, Next >, Cancel

**Screenshot 3: Step 3 - Provide Contact Info**

- Progress bar: 1 Choose User Type, 2 Specify Login Credential, 3 Provide Contact Info, 4 Provide Extra Info
- Fields:
  - Email Address: twhite@example.com
  - ☒ SMS
  - Phone Number: 555555555
  - Service Type: FortiGuard Messaging Service
- Buttons: < Back, Next >, Cancel

**Screenshot 4: Step 4 - Provide Extra Info**

- Progress bar: 1 Choose User Type, 2 Specify Login Credential, 3 Provide Contact Info, 4 Provide Extra Info
- Options:
  - ☒ Enable
  - ☐ Two-factor Authentication
  - ☐ User Group
- Buttons: < Back, Done, Cancel

**Final Step: Assigning User to Group**

- Name: sslvpn\_group
- Type: ☒ Firewall, ☐ Fortinet Single Sign-On (FSSO), ☐ Guest, ☐ RADIUS Single Sign-On (RSSO)
- Available Users:
  - Local Users - guest
- Members:
  - Local Users - twhite

# Adding an address for the network

Go to **Firewall Objects > Address > Addresses**.

Add the address for the local network. Set **Type** to **Subnet**, **Subnet/ IP Range** to the local subnet, and **Interface** to an internal port.

# Adding security policies for access to the Internet and internal network

Go to **Policy > Policy > Policy**.

Add a security policy allowing access to the internal network. Set **Type** to **VPN** and **Subtype** to **SSL-VPN**.



If your FortiGate unit does not have the Policy-based IPsec feature turned on, you will only have to set **Policy Type** to **VPN**.

Set **Incoming Interface** to your Internet-facing interface, **Local Interface** to an internal port and **Local Protected Subnet** to the address for the local network. Create a new **Authentication Rule** to allow the remote user group access.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Show in Address List

☒

Comments

Write a comment... 0/255

Policy Type

☐ Firewall ☒ VPN

Policy Subtype

☐ IPsec ☒ SSL-VPN

Incoming Interface

wan1

Remote Address

all

Local Interface

port1

Local Protected Subnet

Local LAN

☐ SSL Client Certificate Restrictive

Cipher Strength

Any

Configure SSL-VPN Authentication Rules

Create New Edit Delete

User/Group	Service	Schedule	UTM Security	SSL-VPN Portal	Logging	Action
sslvpn_group	ALL	always	-	full-access		✓ ACCEPT
ANY	ALL	always	-			✗ DENY

Tags

Applied tags

Add tag

Comments

Write a comment... 0/1023

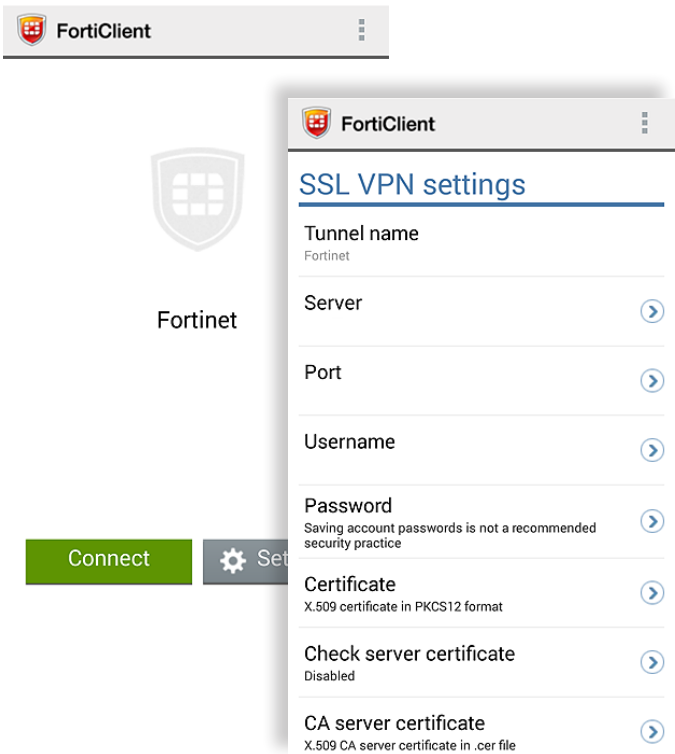
Add a second security policy allowing access to the Internet.

For this policy, **Incoming Interface** is *sslvpn tunnel interface* and **Outgoing Interface** is your Internet-facing interface.

## Configuring the tunnel on FortiClient for Android

Open FortiClient on your Android device and press **Settings**.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	sslvpn tunnel interface
Source Address	SSLVPN_TUNNEL_ADDR1
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	



Select **Server** to configure the server address.

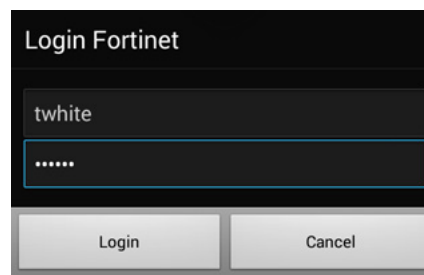
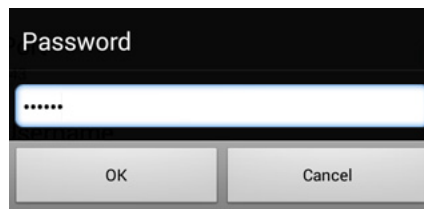
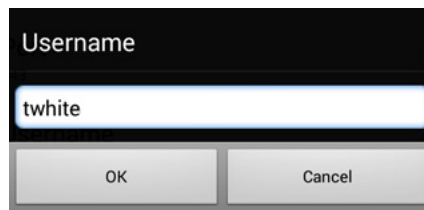
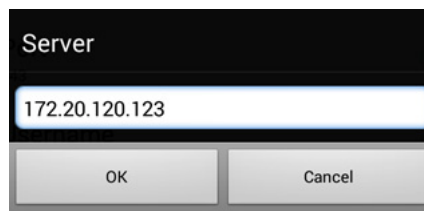


If you changed the default SSL VPN port in the FortiGate, you must also change the **Port** setting on the Android device. Otherwise, leave the port as default.

Next, enter the **Username** and **Password** that you configured on the FortiGate.

Return to the main screen and press the **Connect** button.

Confirm the server connection and press the **Login** button.



FortiClient attempts to establish an SSL VPN tunnel with the FortiGate.

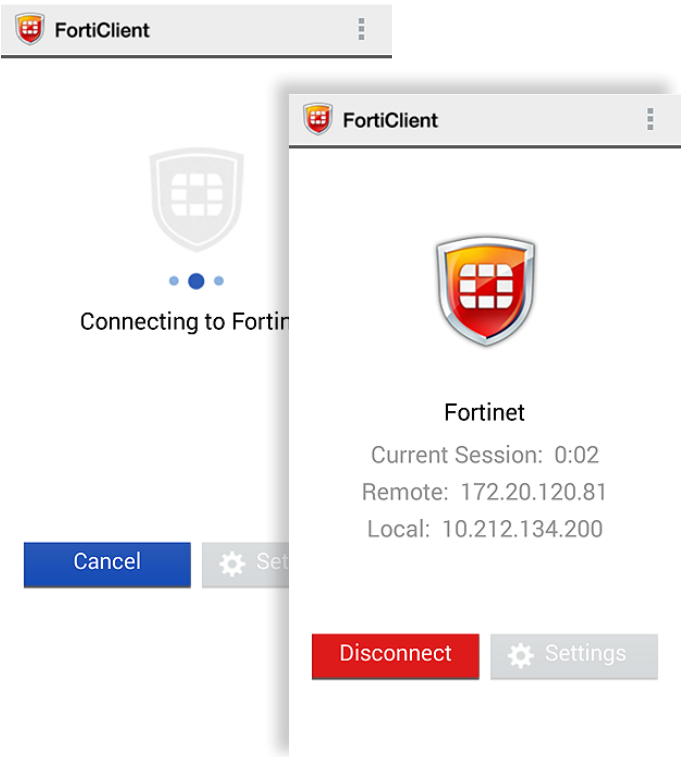
Once the SSL VPN tunnel is active, FortiClient shows the remote and local endpoints, and the duration of the current session.

With the tunnel active, the Android user can start their phone’s mail client or web browser and see content on the protected network.

To close the tunnel, press the **Disconnect** button.

On the FortiGate, verify the connection by navigating to **VPN > Monitor > SSL-VPN** and verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.







User	Source IP	Begin Time	Description
twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession		Tunnel IP:10.212.134.200	









Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.



Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

Select an entry to view more information.

Dst	192.168.1.114	Virtual Domain	root
Received	326664	Source Country	Reserved
Sent / Received	54.36 KB / 319.01 KB	Duration	83
Sent	55665	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	
Timestamp	Wed Apr 17 14:17:15 2013	Tran Display	noop
Sequence Number	3618	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	329
Level	notice 	VPN Type	sslvpn
Src Port	53820	Log ID	13
Sub Type	forward	Threat	
Received Packets	407	Date/Time	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

 Refresh  Download Raw Log					
#	▼ Date/Time	▼ Src Interface	▼ Dst Interface	▼ Src	▼ Dst
▶ 1	14:26:05	ssl.root	wan1	10.212.134.200	 74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	 173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	 66.171.121.34 (fortinet.c
5	14:25:57	ssl.root	wan1	10.212.134.200	 74.121.50.17 (www.page
6	14:25:44	ssl.root	wan1	10.212.134.200	 208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30

Dst	 66.171.121.34 (fortinet.com)	Virtual Domain	root
Received	938	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	535 B / 938 B
Duration	17	Sent	535
Src NAT Port	54165	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65389	Status	close
Timestamp	Wed Apr 17 14:26:03 2013	Tran Display	snat
Sequence Number	8096	Policy ID	8
Src Interface	ssl.root	Src	10.212.134.200
Sent Packets	6	Level	notice 
Src Port	54165	Log ID	13
Sub Type	forward	Threat	
Received Packets	5	Date/Time	14:26:03 (Wed Apr 17 14:26:03 2013)
Dst Interface	wan1		



# Configuring SSL VPN with strong authentication using certificates

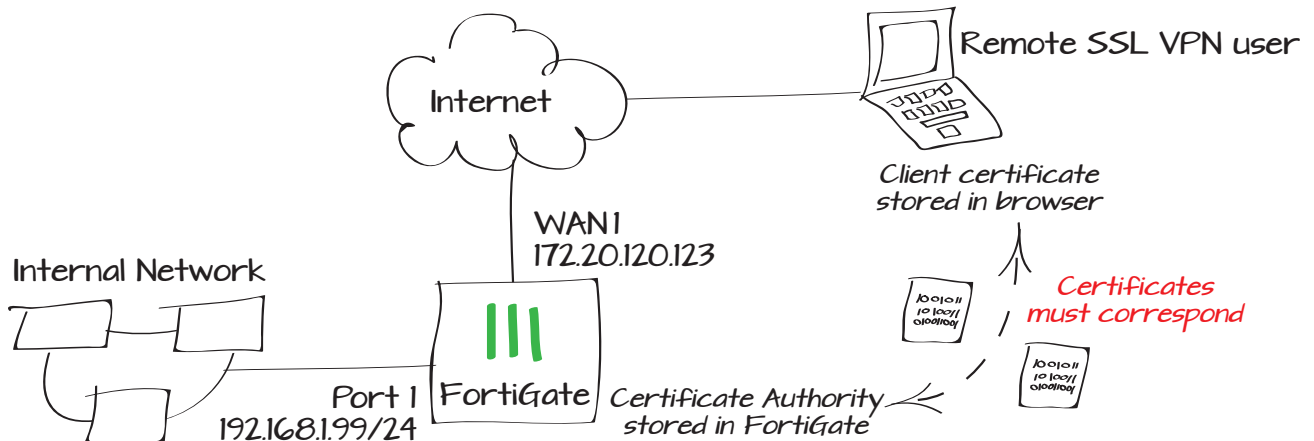
The FortiGate unit can require SSL VPN users to authenticate using a certificate. Similarly, the client can require the FortiGate unit to authenticate using a certificate. The client browser must have a local certificate installed, and the FortiGate unit must have the corresponding CA certificate installed.

This example includes requiring client authentication as well as enabling FortiGate unit authentication.



This example assumes that the correct CA certificate is installed on the FortiGate, and that the client browser has a corresponding local certificate.

1. Creating an SSL VPN tunnel for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Adding security policies for access to the Internet and internal network
5. Configuring the SSL VPN server certificate
6. Results



## Creating an SSL VPN tunnel for remote users

Go to **VPN > SSL > Portal**.

Edit the full-access portal.

The full-access portal allows the use of tunnel mode and/or web mode. In this example you will use both modes.

**Enable Split Tunneling** is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

## Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the User Creation Wizard (in the example, 'twhite').

The screenshot displays the FortiGate User Creation Wizard, a multi-step process for adding a new user. It consists of four steps: 1. Choose User Type, 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info.

**Step 1: Choose User Type**

- ☒ Local User
- ☐ Remote RADIUS User
- ☐ Remote TACACS+ User
- ☐ Remote LDAP User

Buttons: < Back, Next >, Cancel

**Step 2: Specify Login Credential**

User Name:

Password:

Buttons: < Back, Next >, Cancel

**Step 3: Provide Contact Info**

Email Address:

☒ SMS

Phone Number:

Service Type:

Buttons: < Back, Next >, Cancel

**Step 4: Provide Extra Info**

☒ Enable

☐ Two-factor Authentication

☐ User Group

Buttons: < Back, Done, Cancel

Go to **User & Device > User > User Groups**.

Add the user to a user group for SSL VPN connections.

## Adding an address for the local network

Go to **Firewall Objects > Address > Addresses**.

Add the address for the local network. Set **Type** to *Subnet*, **Subnet/ IP Range** to the local subnet, and **Interface** to an internal port.

## Adding security policies for access to the Internet and internal network

Go to **Policy > Policy > Policy**.

Add a security policy allowing access to the internal network. Set **Type** to *VPN* and **Subtype** to **SSL-VPN**.

Set **Incoming Interface** to your Internet-facing interface, **Local Interface** to an internal port and **Local Protected Subnet** to the address for the local network.

Create a new **Authentication Rule** to allow the remote user group access.

Enable **SSL Client Certificate Restrictive**.

Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Available Users

- Local Users - guest

Members

- Local Users - twwhite

Category ☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List ☒

Comments  0/255

Policy Type ☐ Firewall ☒ VPN

Policy Subtype ☐ IPsec ☒ SSL-VPN

Incoming Interface

Remote Address  +

Local Interface

Local Protected Subnet  +

☒ SSL Client Certificate Restrictive

Cipher Strength

### Configure SSL-VPN Authentication Rules

Create New	Edit	Delete				
User/Group	Service	Schedule	UTM Security	SSL-VPN Portal	Logging	Action
sslvpn_group twwhite	ALL	always	-	full-access		ACCEPT
ANY	ALL	always	-			DENY



You *must* enable the **SSL Client Certificate Restrictive** checkbox or certificates will not be required for the tunnel.

Add a second security policy allowing access to the Internet.

For this policy, **Incoming Interface** is *sslvpn tunnel interface* and **Outgoing Interface** is your Internet-facing interface.

## Configuring the SSL VPN server certificate

Go to **VPN > SSL > Config**.

Select the desired server certificate and enable Require Client Certificate.



You *must* enable the **Require Client Certificate** checkbox or certificates will not be required for the tunnel.

Optionally, set the **Encryption Key Algorithm**, **Idle Timeout**, and **Login Port** as desired.

## Results

On the remote client, attempt to connect to the SSL VPN tunnel using a web browser or FortiClient.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	sslvpn tunnel interface
Source Address	SSLVPN_TUNNEL_ADDR1
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	

IP Pools

SSLVPN\_TUNNEL\_ADDR1

Server Certificate	Fortinet_CA_SSLProxy
Require Client Certificate	<input checked="" type="checkbox"/>
Encryption Key Algorithm	<input type="radio"/> High - AES(128/256 bits) and 3DES <input checked="" type="radio"/> Default - RC4(128 bits) and higher <input type="radio"/> Low - RC4(64 bits), DES and higher
Idle Timeout	300 (seconds)
Login Port	10443
<input type="checkbox"/> Allow Endpoint Registration (Tunnel Mode Only)	

# Using a web browser

Enter the tunnel IP into your web browser's address bar.

If the client certificate has not yet been installed in the browser, you will be prompted by a warning message.

If you are absolutely certain that this is the IP you wish to connect to, click **Proceed anyway** to accept the certificate. Otherwise, click **Back to safety** (these options may vary from browser to browser).

Once the browser acknowledges the FortiGate certificate, you will be presented with a web portal login screen.

Enter the username and password associated with the VPN and click **Login**.

The web portal opens and displays the session information and any bookmarks that may have been assigned.

Use this portal to connect to the SSL VPN tunnel. Under Tunnel Mode, click **Connect**.

The connection is successful when the **Link status** is 'Up' and traffic flows.



## This is probably not the site you are looking for!

You attempted to reach 209.87.254.222, but instead you actually reached a server identifying itself as FGT1KC3912801463. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of 209.87.254.222

You should not proceed, **especially** if you have never seen this warning before for this site.

[Proceed anyway](#) [Back to safety](#)

[Help me understand](#)

### Please Login

**Name:**

**Password:**

Welcome to SSL-VPN Service

HelpLogout

#### Session Information

Time Logged In:	psheng(0 hour(s), 0 minute(s), 41 second(s))
HTTP Inbound/Outbound Traffic:	0 bytes / 0 bytes
HTTPS Inbound/Outbound Traffic:	0 bytes / 0 bytes

#### Bookmarks

#### Connection Tool

Type:

HTTP/HTTPS

Host:

#### FortiClient Download

[FortiClient iOS](#)[FortiClient Android](#)

#### Tunnel Mode

Link status:Up

Bytes sent:21845

Bytes received:16322

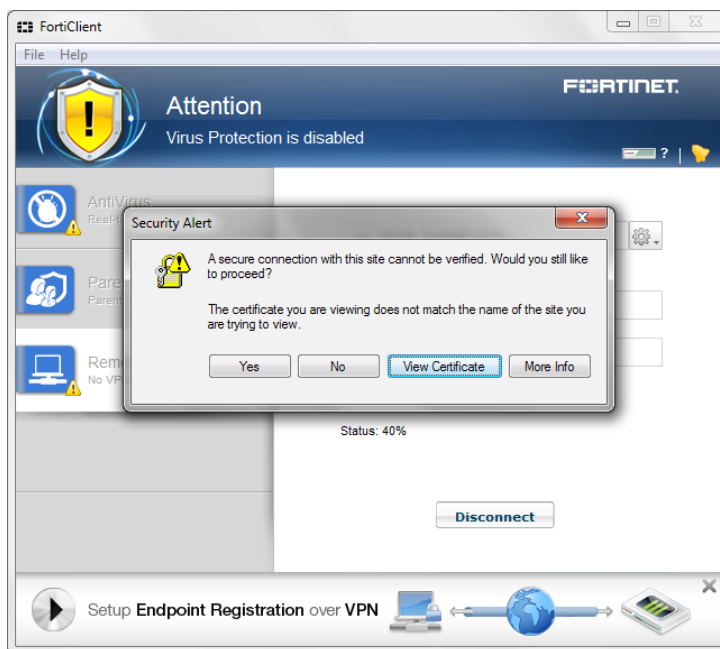
## Using FortiClient

Open the FortiClient application and create a new SSL VPN connection.

When connecting to this tunnel the first time, you are presented with a security alert asking whether or not to trust the certificate.

To install the certificate permanently, click **View Certificate > Install Certificate**.

Follow the Certificate Import Wizard. Click **Next**.



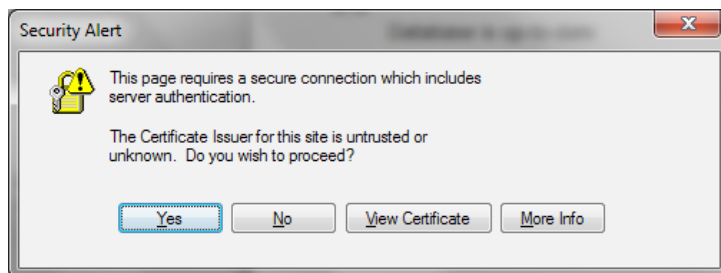
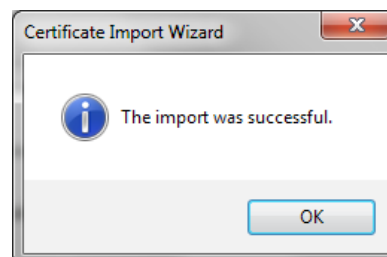
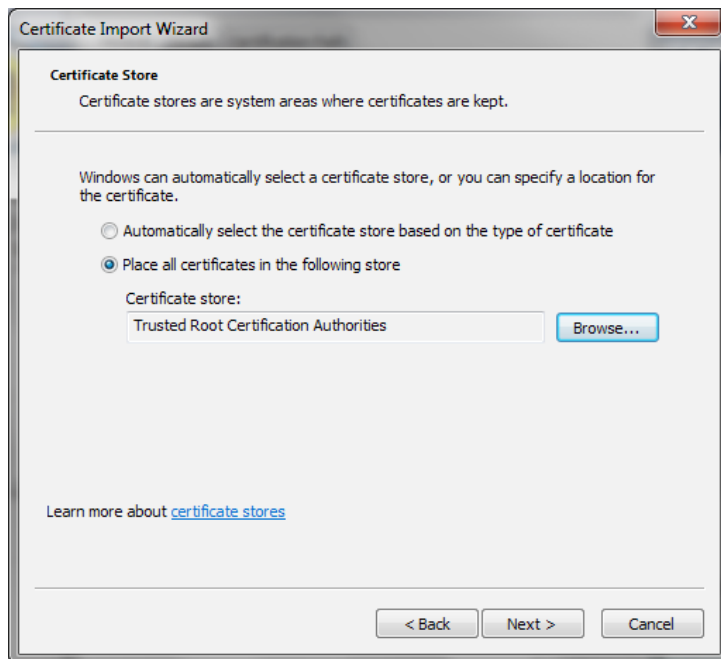
When the wizard asks you which store to place the certificate in, browse to and select the **Trusted Root Certification Authorities** store.

Click **Next**, confirm the import options, and click **Finish**. The wizard will inform you that the certificate imported successfully.

Click **OK** until you are back at the security alert and click **Yes**.

The tunnel should now activate.

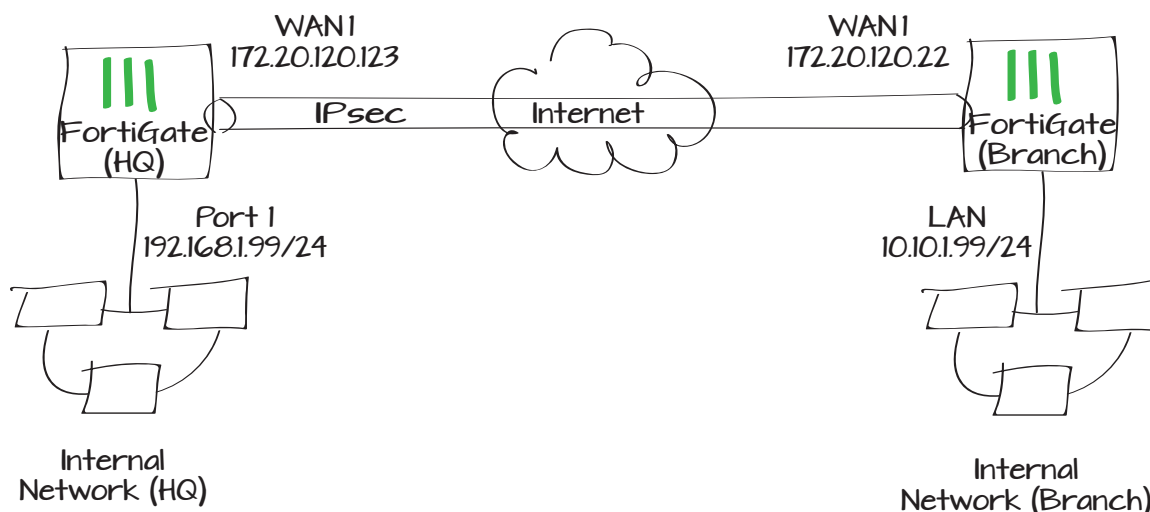
The next time you connect to this tunnel you won't need to reimport the certificate, unless of course you imported it incorrectly the first time.



# Using IPsec VPN to provide communication between offices

This example provides secure, transparent communication between two FortiGates located at different offices using route-based IPsec VPN. In this example, one office will be referred to as HQ and the other will be referred to as Branch.

1. Configuring the HQ IPsec VPN
2. Adding firewall addresses for the local and remote LAN on HQ
3. Creating an HQ security policy and static route
4. Configure the Branch IPsec VPN Phase 1 and Phase 2 settings
5. Add Branch firewall addresses for the local and remote LAN
6. Create a branch IPsec security policy and static route
7. Results





# Configuring the HQ's IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the Branch FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.

Name

To\_Branch\_Net

Comments

Write a comment...

0/255

Remote Gateway

Static IP Address

IP Address

172.20.120.22

Local Interface

wan1

Mode

☐ Aggressive

☒ Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

☒ Accept any peer ID

IKE Version

☒ 1

☐ 2

Mode Config

☐

Local Gateway IP

☒ Main Interface IP

☐ Specify

0.0.0.0

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

☐ 1

☐ 2

☒ 5

☐ 14

Keylife

28800

(120-172800 seconds)

Local ID

(optional)

XAUTH

☒ Disable

☐ Enable as Client

☐ Enable as Server

NAT Traversal

☒ Enable

Keepalive Frequency

10

(10-900 seconds)

Dead Peer Detection

☒ Enable

Using IPsec VPN to provide communication between offices

345

Now select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the HQ subnet and **Destination address** as the Branch subnet.

Adding firewall addresses for the local and remote LAN on HQ

Go to **Firewall Objects > Address > Addresses**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to an internal port.

Name

To\_Branch\_Net\_Phase2

Comments

Write a comment...

0/255

Phase 1

To\_Branch\_Net

Advanced...

P2 Proposal

1- Encryption: 3DES Authentication: SHA1

2- Encryption: AES128 Authentication: SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife:

Seconds

1800

(Seconds)

5120

(KBytes)

Autokey Keep Alive

☐ Enable

Auto-negotiate

☐ Enable

Quick Mode Selector

Source address

☐ Specify 192.168.1.0/24

☐ Select -----Address-----

Source port

0

Destination address

☐ Specify 10.10.1.0/24

☐ Select -----Address-----

Destination port

0

Protocol

0

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Show in Address List

☒

Comments

Write a comment...

0/255

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to the VPN Phase 1.

## Creating an HQ security policy and static route.

Go to **Policy > Policy > Policy**.

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.

Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	Remote LAN
Color	[Change]
Type	Subnet
Subnet / IP Range	10.10.1.0/255.255.255.0
Interface	To_Branch_Net
Show in Address List	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> SSL-VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	port1
Source Address	Local LAN
Outgoing Interface	To_Branch_Net
Destination Address	Remote LAN
Schedule	always
Service	ALL
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> SSL-VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	To_Branch_Net
Source Address	Remote LAN
Outgoing Interface	port1
Destination Address	Local LAN
Schedule	always
Service	ALL
Action	ACCEPT
<input type="checkbox"/> Enable NAT	

Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.



If the **Router** menu is not visible, go to **System > Config > Features** to ensure that **Advanced Routing** is turned on.

## Configuring the Branch's IPsec VPN

On the Branch FortiGate, Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the HQ FortiGate, **Local Interface** to the Internet-facing interface, and enter the same **Pre-shared Key** used previously.

Destination IP/Mask	<input type="text" value="10.10.1.0/255.255.255.0"/>		
Device	<input type="text" value="To_Branch_Net"/>		
Distance	<input type="text" value="5"/>	(1-255, Default=10)	
Priority	<input type="text" value="0"/>	(0-4294967295)	
Comments	<input type="text" value="Write a comment..."/>		0/255

Name	<input type="text" value="To_HQ_Net"/>		
Comments	<input type="text" value="Write a comment..."/>		0/255
Remote Gateway	<input type="text" value="Static IP Address"/>		
IP Address	<input type="text" value="172.20.120.123"/>		
Local Interface	<input type="text" value="wan1"/>		
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)		
Authentication Method	<input type="text" value="Preshared Key"/>		
Pre-shared Key	<input type="text" value="....."/>		

**Peer Options**

☒ Accept any peer ID

IKE Version ☒ 1 ☐ 2

Mode Config ☐

Local Gateway IP ☒ Main Interface IP ☐ Specify

<b>P1 Proposal</b>			
1 - Encryption	<input type="text" value="3DES"/>	Authentication	<input type="text" value="SHA1"/>
2 - Encryption	<input type="text" value="AES128"/>	Authentication	<input type="text" value="SHA1"/>
DH Group	1 <input type="checkbox"/> 2 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 14 <input type="checkbox"/>		
Keylife	<input type="text" value="28800"/>	(120-172800 seconds)	
Local ID	<input type="text"/>	(optional)	
<b>XAUTH</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable as Client <input type="radio"/> Enable as Server		
NAT Traversal	<input checked="" type="checkbox"/> Enable		
Keepalive Frequency	<input type="text" value="10"/>	(10-900 seconds)	
<b>Dead Peer Detection</b>	<input checked="" type="checkbox"/> Enable		

Now select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the Branch subnet and **Destination address** as the HQ subnet.

Adding firewall addresses for the local and remote LAN on HQ

Go to **Firewall Objects > Address > Addresses.**

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to an internal port.

Name

To\_HQ\_Net\_Phase2

Comments

Write a comment...

0/255

Phase 1

To\_HQ\_Net

Advanced...

P2 Proposal

1- Encryption: 3DES Authentication: SHA1

2- Encryption: AES128 Authentication: SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife:

Seconds

1800

(Seconds)

5120

(KBytes)

Autokey Keep Alive

☐ Enable

Auto-negotiate

☐ Enable

Quick Mode Selector

Source address

☐ Specify 10.10.1.0/24

☐ Select -----Address-----

Source port

0

Destination address

☐ Specify 192.168.1.0/24

☐ Select -----Address-----

Destination port

0

Protocol

0

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

10.10.1.0/255.255.255.0

Interface

lan

Show in Address List

☒

Comments

Write a comment...

0/255

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to the VPN Phase 1.

## Creating an HQ security policy and static route.

Go to **Policy > Policy > Policy**.

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.

Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Remote LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

To\_HQ\_Net

Show in Address List

☒

Comments

Write a comment... 0/255

Policy Type

☒ Firewall ☐ SSL-VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

lan

Source Address

Local LAN

Outgoing Interface

To\_HQ\_Net

Destination Address

Remote LAN

Schedule

always

Service

ALL

Action

ACCEPT

☐ Enable NAT

Policy Type

☒ Firewall ☐ SSL-VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

To\_HQ\_Net

Source Address

Remote LAN

Outgoing Interface

lan

Destination Address

Local LAN

Schedule

always

Service

ALL

Action

ACCEPT

☐ Enable NAT

Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.

## Results

Go to **VPN > Monitor > IPSec Monitor** to verify the status of the VPN tunnel. It should be up.

A user on either of the office networks should be able to connect to any address on the other office network transparently.

From the HQ FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic** to verify that both inbound and outbound traffic is occurring.

To verify traffic on the Branch FortiGate unit as well, go to **Log & Report > Traffic Log > Forward Traffic**.

Destination IP/Mask	<input type="text" value="192.168.1.0/255.255.255.0"/>
Device	<input type="text" value="To_HQ_Net"/>
Distance	<input type="text" value="5"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

Status	Incoming Data	Outgoing Data	
<a href="#">Bring Down</a>	2232 B	1725 B	1

#	Date/Time	Src Interface	Dst Interface
1	15:17:47	To_Branch_Net	port1
2	15:17:43	port1	To_Branch_Net
3	15:17:32	To_Branch_Net	port1

#	Date/Time	Src	Dst
1	15:12:30	192.168.1.116	10.10.1.200
2	15:10:12	192.168.1.116	10.10.1.200
3	15:07:47	10.10.1.200	192.168.1.114
4	15:05:45	10.10.1.200	192.168.1.114
5	15:04:28	10.10.1.200	192.168.1.114
6	14:40:08	10.10.1.200	192.168.1.114

## Extra help: IPsec VPN

This section contains tips to help you with some common challenges of IPsec VPNs.

The options to configure policy-based IPsec VPN are unavailable.

Go to **System > Config > Features**. Select **Show More** and turn on **Policy-based IPsec VPN**.

The VPN connection attempt fails.

If your VPN fails to connect, check the following:

- Ensure that the pre-shared keys match exactly.
- Ensure that both ends use the same P1 and P2 proposal settings.
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.
- Ensure that your FortiGate unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly on the FortiGate and that clients have specified the correct Local ID.
- If you are using FortiClient, ensure that your version is compatible with the FortiGate firmware by reading the [FortiOS Release Notes](#).
- Ensure that the Quick Mode selectors are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range.



- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the FortiGate unit is set to **Enable as Server**.
- If your FortiGate unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your FortiGate unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the diagnostic command in the CLI:

```
diag debug application ike -1
diag debug enable
```

The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

```
diag debug reset
diag debug disable
```

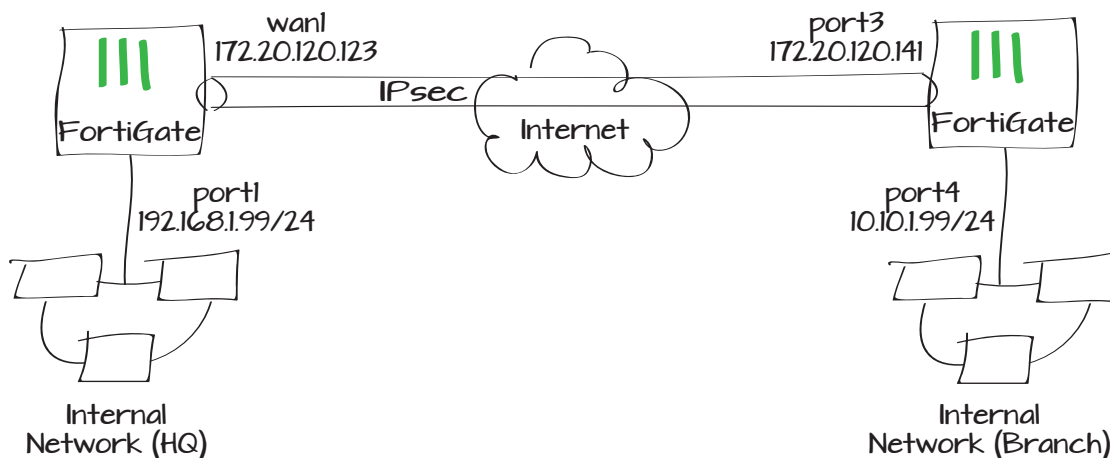
### The VPN tunnel goes down frequently.

If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.

# Using policy-based IPsec VPN for communication between offices

This example uses policy-based IPsec VPN, and assumes that both offices have connections to the Internet with static IP addresses. In this example, one FortiGate unit will be called HQ and the other will be called Branch.

1. Enabling policy-based VPN on the HQ FortiGate unit
2. Configuring the HQ IPsec VPN Phase 1 and Phase 2 settings
3. Adding the HQ firewall addresses for the local and remote LAN
4. Creating an HQ IPsec security policy
5. Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings
6. Adding Branch firewall addresses for the local and remote LAN
7. Creating a branch IPsec security policy
8. Results



## Enabling policy-based VPN on the HQ FortiGate unit

Go to **System > Config > Features**. Select **Show More** and turn on **Policy-based IPsec VPN**.

NAT46 & NAT64

OFF

Policy-based IPsec VPN

ON

SSL-VPN Custom Login Page

OFF

Changes:

✓ Policy-based IPsec VPN  
Disabled -> Enabled

Apply Reset

## Configuring the HQ IPsec VPN Phase 1 and Phase 2 settings

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the Branch FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.

Name

Comments  0/255

Remote Gateway

IP Address

Local Interface

Mode ☐ Aggressive ☒ Main (ID protection)

Authentication Method

Pre-shared Key

Peer Options

☒ Accept any peer ID

IKE Version ☒ 1 ☐ 2

Mode Config ☐

Local Gateway IP ☒ Main Interface IP ☐ Specify

**P1 Proposal**

1 - Encryption  Authentication

2 - Encryption  Authentication  ☒ ☐

DH Group ☐ 1 ☐ 2 ☒ 5 ☐ 14

Now select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the HQ subnet and **Destination address** as the Branch subnet.

Adding HQ addresses for the local and remote LAN on the HQ FortiGate unit

Go to **Firewall Objects > Address > Address**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to an internal port.

Name

HQ\_to\_Branch\_P2

Comments

Write a comment...

0/255

Phase 1

HQ\_to\_Branch\_P1

Advanced...

P2 Proposal

1- Encryption: 3DES Authentication: SHA1

2- Encryption: AES128 Authentication: SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife:

Seconds 1800 (Seconds) 5120 (KB)

Autokey Keep Alive

☐ Enable

Quick Mode Selector

Source address

☐ Specify 192.168.1.0/24

☐ Select -----Address-----

Source port

0

Destination address

☐ Specify 10.10.1.0/24

☐ Select -----Address-----

Destination port

0

Protocol

0

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port1

Show in Address List

☒

Comments

Write a comment...

0/255

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to the Internet-facing interface.

## Creating an HQ IPsec security policy

Go to **Policy > Policy > Policy**.

Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	Remote LAN
Color	[Change]
Type	Subnet
Subnet / IP Range	10.10.1.0/255.255.255.0
Interface	wan1
Show in Address List	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

Policy Type	<input type="radio"/> Firewall <input checked="" type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> IPsec <input type="radio"/> SSL-VPN
Local Interface	port1
Local Protected Subnet	Local LAN
Outgoing VPN Interface	wan1
Remote Protected Subnet	Remote LAN
Schedule	always
Service	ALL
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>VPN Tunnel</b>	
<input type="radio"/> Create New <input checked="" type="radio"/> Use Existing	
VPN Tunnel HQ_to_Branch_P1	
<input checked="" type="checkbox"/> Allow traffic to be initiated from the remote	

# Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the HQ FortiGate, **Local Interface** to the Internet-facing interface, and enter the same **Pre-shared Key** used in the HQ Phase 1.

Select **Create Phase 2**, set it to use the new Phase 1, and expand the **Advanced** options.

Specify **Source address** as the Branch subnet and **Destination address** as the HQ subnet.

Name

Branch\_to\_HQ\_P1

Comments

Write a comment...

0/255

Remote Gateway

Static IP Address

IP Address

172.20.120.123

Local Interface

lan

Mode

Aggressive

Main (ID protection)

Authentication Method

port3 (External Interface)

Pre-shared Key

Peer Options

Accept any peer ID

IKE Version

1

2

Mode Config

Local Gateway IP

Main Interface IP

Specify

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1

2

5

14

Name

Branch\_to\_HQ\_P2

Comments

Write a comment...

0/255

Phase 1

Branch\_to\_HQ\_P1

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group

1

2

5

14

Keylife:

Seconds

1800

(Seconds)

5120

(KBytes)

Autokey Keep Alive

Enable

Quick Mode Selector

Source address

Specify

10.10.1.0/24

Select

-----Address-----

Source port

0

Destination address

Specify

192.168.1.0/24

Select

-----Address-----

Destination port

0

Protocol

0

# Adding Branch addresses for the local and remote LAN on the HQ FortiGate unit

Go to **Firewall Objects > Address > Address**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to an internal port.

Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to the Internet-facing interface.


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Local LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

10.10.1.0/255.255.255.0

Interface

port4 (Internal Interface)

Show in Address List

☒

Comments

Write a comment... 0/255


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Remote LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

192.168.1.0/255.255.255.0

Interface

port3 (External Interface)

Show in Address List

☒

Comments

Write a comment... 0/255

# Creating a Branch IPsec security policy

Go to **Policy > Policy > Policy**.

Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.

## Results

Go to **VPN > Monitor > IPsec Monitor** to verify the status of the VPN tunnel. It should be up.

A user on either of the office networks should be able to connect to any address on the other office network transparently.

From the HQ FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic**.

From the Branch FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic**.

Policy Type

Firewall

VPN

Policy Subtype

IPsec

SSL-VPN

Local Interface

port4 (Internal Interface)

Local Protected Subnet

Local LAN

Outgoing VPN Interface

port3 (External Interface)

Remote Protected Subnet

Remote LAN

Schedule

always

Service

ALL

Logging Options

No Log

Log Security Events

Log all Sessions

VPN Tunnel

Create New

Use Existing

VPN Tunnel

Branch\_to\_HQ\_P1

Allow traffic to be initiated from the remote site

Name	Remote Gateway	Proxy ID Source	Proxy ID Destination	Status	Incoming
to_Branch_P1	172.20.120.141	192.168.1.0/24	10.10.1.0/24	<span>Bring Down</span>	23664 E

Src	Dst	Sent / Received	Policy ID	Service	VPN	VPN
192.168.1.117	208.91.112.50	304 B / 304 B	3	ALL_UDP_CUSTOM		
192.168.1.114	10.10.1.100	1.08 KB / 1.24 KB	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.113.70	1.19 KB / 1.19 KB	3	ALL_UDP_CUSTOM		
172.20.120.141	172.20.120.125	1.79 KB / 1.90 KB	5	RDP		
10.10.1.100	192.168.1.114	468 B / 1.29 KB	11	ALL_UDP_CUSTOM	HQ_to_Branch_P1	ipsec-sta
10.10.1.100	192.168.1.114	516 B / 876 B	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.112.53	3.26 KB / 10.00 KB	3	ALL_UDP_CUSTOM		
10.10.1.100	192.168.1.150	441 B / 525 B	11	12101/udp	HQ_to_Branch_P1	ipsec-sta

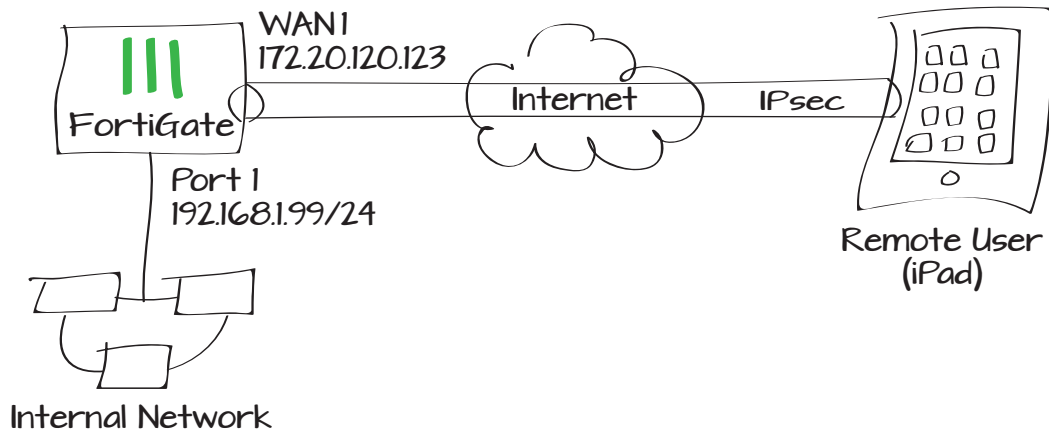
Date/Time	Src	Dst	Sent / Received	Policy ID	Service	VPN
09:57:05	10.10.1.100	172.20.181.32	0 B / 0 B	1	57622/udp	
09:56:57	10.10.1.100	111.221.77.146	0 B / 0 B	1	40039/udp	
09:56:57	10.10.1.100	157.55.235.154	0 B / 0 B	1	40042/udp	
09:56:55	10.10.1.100	192.168.1.114	552 B / 276 B	4	PING	Branch_to_H
09:56:35	10.10.1.100	111.221.74.23	0 B / 0 B	1	40045/udp	



# Providing secure remote access to a network for an iOS device

This recipe uses the VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The example enables group members to access the internal network and forces them through the FortiGate unit when accessing the Internet. The example uses an iPad 2 running iOS 6.1.2 (menu options may vary for different iOS versions and devices).

1. Creating a user group for iOS users
2. Adding addresses for the local LAN and remote users
3. Configuring IPsec VPN phases using the VPN Wizard
4. Creating security policies for access to the internal network and the Internet
5. Configuring VPN on the iOS device
6. Results



## Creating a user group for iOS users

Go to **User & Device > User > User Definition**.

Create a new user.

Go to **User & Device > User > User Groups**.

Create a user group for iOS users and add the user you created.

## Adding addresses for the local LAN and remote users

Go to **Firewall Objects > Address > Addresses**.

Add the address for the local network, including the subnet and local interface.

Go to **Firewall Objects > Address > Addresses**.

Add the address for the remote user, including the IP range.

# Configuring the IPsec VPN phases using the VPN Wizard

Go to **VPN > IPSec > Auto Key (IKE)**.

Select **Create VPN Wizard**. Name the VPN connection and select **Dial Up - iPhone / iPad Native IPsec Client**. Click **Next**.

Enter your pre-shared key and select the iOS user group, then click **Next**. Note that the pre-shared key is a credential for the VPN and should differ from the user's password.

Select your Internet-facing interface for the **Local Outgoing Interface**, and enter the IP range from the address range you created.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

ios\_users

Color

[Change]

Type

IP Range

Subnet / IP Range

10.10.1.100-10.10.1.110

Interface

Any

Show in Address List

☒

Comments

Write a comment... 0/255

1 VPN Setup

2 Authentication

3 Network

Name

ios\_P1

VPN Type

☐ Dial Up - FortiClient Windows, Mac and Android

☒ Dial Up - iPhone / iPad Native IPsec Client

< Back

Next >

Cancel

1 VPN Setup

2 Authentication

3 Network

Pre-shared Key

.....

User Group

ios\_group

< Back

Next >

Cancel

1 VPN Setup

2 Authentication

3 Network

Local Outgoing Interface

wan1

Address Range

10.10.1.100-10.10.1.110

Subnet Mask

255.255.255.0

DNS Server

☒ Use System DNS

☐ Specify

☐ Enable IPv4 Split Tunnel

< Back

Done

Cancel

# Assigning an IP to the VPN interface (optional)

If you wish to control the IP address that will be assigned to any traffic egressing over the IPsec interface, you can assign an IP to the interface.

Go to **System > Network > Interfaces**. Expand your Internet-facing interface and edit the VPN interface.

Assign the **IP** and **Remote IP** addresses. These addresses should not be related to the IPs used for the internal network or the Internet-facing interface.

Name	ios_P1
Type	Tunnel Interface
Interface	wan1

---

Addressing mode	Manual
IP	10.10.80.1
Remote IP	172.16.2.5
IPv6 Address	::/0

# Creating security policies for access to the internal network and the Internet

Go to **Policy > Policy > Policy**.

Create a security policy allowing remote iOS users to access the internal network.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	ios_P1
Source Address	all
Outgoing Interface	port1
Destination Address	Local LAN
Schedule	always
Service	ALL
Action	✓ ACCEPT

Go to **Policy > Policy > Policy**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit. Ensure that **Enable NAT** is checkmarked.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

ios\_P1

Source Address

all

Outgoing Interface

wan1

Destination Address

all

Schedule

always

Service

ALL

Action

ACCEPT

☒ Enable NAT

☒ Use Destination Interface Address ☐ Fixed Port

☐ Use Dynamic IP Pool

Click to add...

## Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.



In order to connect to the VPN tunnel, a **Group Name** may be required. If you are unable to connect, add this field to the VPN client to determine if the blank field is the cause.

Description

To-Office-VPN

Server

172.20.120.123

Account

twhite

Password

.....

Use Certificate

☐ OFF

Group Name

Secret

.....

# Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Select an entry to view more information.

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log >**

Name	Type	Remote Gateway	Username	Proxy ID Sour
ios_P1_0	Dialup	172.20.120.126	twhite	0.0.0.0-255.255.255.

<div>RefreshDownload Raw Log</div>							
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received	
1	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	59 B / 221 B	7
2	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	60 B / 292 B	7
3	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	56 B / 288 B	7
4	11:21:42	port1	wan1	192.168.1.117	208.91.113.70	304 B / 304 B	3
5	11:20:44	ios_P1	port1	10.10.1.100	192.168.1.114	72 B / 72 B	6

Dst	192.168.1.114	Virtual Domain	root
Received	72	Source Country	Reserved
Sent / Received	72 B / 72 B	Duration	63
Sent	72	Application Details	
Service	PING	Protocol	1
Destination Country	Reserved	roll	65428
Status	✓	Timestamp	Thu Feb 21 11:20:44 2013
Tran Display	noop	Sequence Number	220067
Policy ID	6	Src Interface	ios_P1
Src	10.10.1.100	VPN	ios_P1_0
Sent Packets	2	Level	notice
VPN Type	ipsec-dynamic	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:20:44 (Thu Feb 21 11:20:44 2013)
Dst Interface	port1		

**Forward Traffic** to view the traffic.

Select an entry to view more information.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received	Policy
1	11:28:43	ios_P1	wan1	10.10.1.100	74.121.50.17	1023 B / 579 B	7
2	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	59 B / 221 B	7
3	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	60 B / 292 B	7
4	11:22:41	ios_P1	wan1	10.10.1.100	208.91.112.53	56 B / 288 B	7
5	11:20:42	ios_P1	wan1	10.10.1.100	173.194.73.105	812 B / 642 B	7

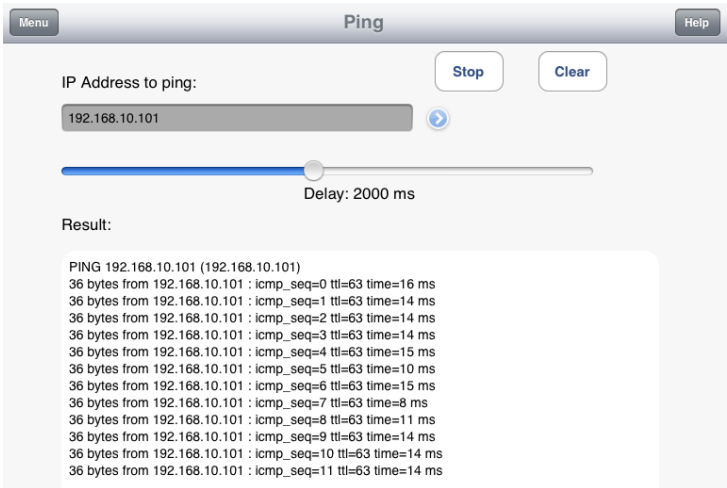
Dst	74.121.50.17	Virtual Domain	root
Received	579	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	1023 B / 579 B
Duration	2	Sent	1023
Src NAT Port	50189	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65428	Status	close
Timestamp	Thu Feb 21 11:28:43 2013	Tran Display	snat
Sequence Number	221594	Policy ID	7
Src Interface	ios_P1	Src	10.10.1.100
VPN	ios_P1_0	Sent Packets	6
Level	notice	VPN Type	ipsec-dynamic
Src Port	50189	logid	13
Sub Type	forward	Threat	
Received Packets	4	Date/Time	11:28:43 (Thu Feb 21 11:28:43 2013)
Dst Interface	wan1		

View the status of the tunnel on the iOS device.

On the iPad, go to **Settings > General > VPN** and view the **Status** of the connection.



Using a Ping tool, send a ping packet directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel..





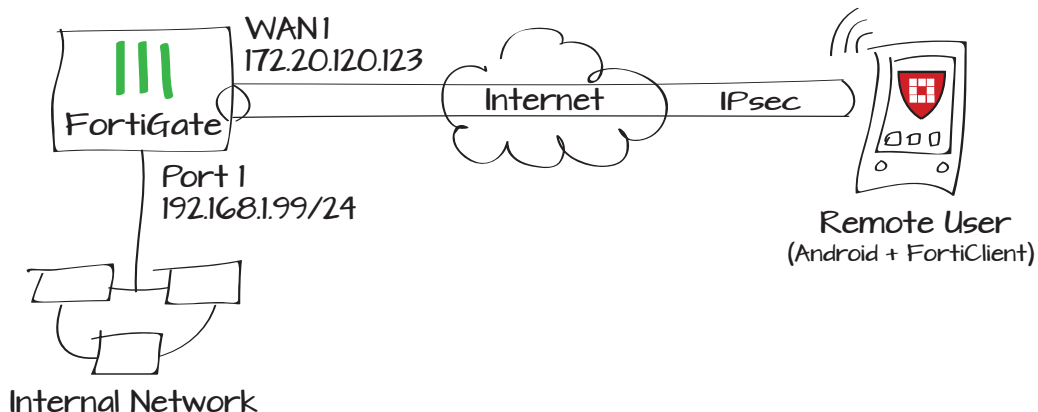
# Connecting an Android to a FortiGate with IPsec VPN

This recipe describes how to provide a group of remote Android users with secure, encrypted access to the network using FortiClient.



You must download the FortiClient application from the Play Store and install it on your Android device. Refer to the [FortiClient for Android QuickStart Guide](#). This recipe was tested using Android version 4.3.

1. Creating a user group for Android users
2. Adding firewall addresses for the user group and DMZ network
3. Configuring the FortiGate as an L2TP server
4. Configuring IPsec VPN using the VPN Wizard
5. Assigning an IP to the VPN interface (optional)
6. Creating a security policy for access to the internal network and the Internet
7. Configuring VPN on the Android device using FortiClient
8. Results



## Creating a user group for Android users

Go to **User & Device > User > User Definition** and select **Create new** to start the user creation wizard.

Add a user for each remote client, specifying the user type and login credentials.

Provide extra information as required and press **OK**.

Go to **User & Device > User > User Groups**.

Create a user group for Android users and add the users you created.

The screenshot shows the 'Specify Login Credential' step of a four-step wizard. The steps are: 1. Choose User Type, 2. Specify Login Credential (active), 3. Provide Contact Info, and 4. Provide Extra Info. The 'User Name' field contains 'bwayne' and the 'Password' field contains eight asterisks. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'User Group' configuration page. The 'Name' field is 'Android\_Users'. The 'Type' section has three radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest'. Below this is the 'Single Sign-On (RSSO)' section with a 'Members' field containing 'bwayne' and a green plus icon. The 'Remote authentication servers' section has a table with columns 'Remote Server' and 'Group Name'. The table is empty with the text 'No matching entries found' in the center. At the bottom are 'OK' and 'Cancel' buttons.

## Adding firewall addresses for the Android user group and the DMZ network

Go to **Firewall Objects > Address > Addresses**.

Select **Create New** and add a firewall address for the Android users.

The screenshot shows the 'Address' configuration page. The 'Name' field is 'Android\_Users'. The 'Type' dropdown is set to 'IP Range'. The 'Subnet / IP Range' field contains '192.168.1.90-192.168.1.99'. The 'Interface' dropdown is set to 'wan1'. The 'Show in Address List' checkbox is checked. The 'Comments' field contains 'Write a comment...' and a character count '0/255'.

Go to **Firewall Objects > Address > Addresses**.

Select **Create New** and add a firewall address for the DMZ network.

## Configuring the FortiGate as an L2TP server

Go to **System > Dashboard > Status** and enter the following in the CLI Console:

Name	<input type="text" value="DMZ_Server"/>
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="10.10.10.0/255.255.255.0"/>
Interface	<input type="text" value="dmz"/>
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

```
config vpn l2tp
    set sip 192.168.1.90
    set eip 192.168.1.99
    set status enable
    set usrgrp Android_Users
end
```

## Configuring IPsec VPN using the VPN Wizard

Go to **VPN > IPsec > Auto Key (IKE)** and select **Create VPN Wizard**.

Select **Dial Up - FortiClient Windows, Mac and Android** and follow the wizard, entering the information that it requests.

1 VPN Setup

2 Authentication

3 Network

4 Client Options

Name	<input type="text" value="AndroidVPN"/>
VPN Type	<div><div><input checked="" type="radio"/> Dial Up - FortiClient Windows, Mac and Android</div><div><input type="radio"/> Dial Up - iPhone / iPad Native IPsec Client</div></div>

< Back

Next >

Cancel

The user group that you select determines who is allowed to connect to this VPN.

Enter the pre-shared key that will also be used on the Android device.

Clients will connect to the FortiGate unit through the WAN1 interface, which is connected to the Internet.

**Address Range** defines the IP address range to assign to clients.

The options on the final wizard page can make the VPN more convenient to use. They are disabled by default.

Go to **VPN > IPsec > Auto Key (IKE)** and edit the AndroidVPN Phase 1.

Set **1 - Encryption** to *AES128* with *SHA1* authentication.

Set **2 - Encryption** to *3DES* with *SHA1* authentication.

VPN Setup

Authentication

Network

Client Options

Authentication Method

Pre-shared Key

RSA Signature

Pre-shared Key

.....

User Group

Android\_Users

< Back

Next >

Cancel

VPN Setup

Authentication

Network

Client Options

Local Outgoing Interface

wan1

Address Range

192.168.1.90-192.168.1.99

Subnet Mask

255.255.255.0

DNS Server

Use System DNS

Specify

Enable IPv4 Split Tunnel

Allow Endpoint Registration

< Back

Next >

Cancel

VPN Setup

Authentication

Network

Client Options

Save Password

Auto Connect

Always Up (Keep Alive)

< Back

Done

Cancel

P1 Proposal

1 - Encryption

AES128

Authentication

SHA1

2 - Encryption

3DES

Authentication

SHA1

DH Group

1

1

2

5

14

Keylife

28800

(120-172800 seconds)

Local ID

(optional)

Go to **VPN > IPsec > Auto Key (IKE)** and edit the Android VPN Phase 2.

Set **1 - Encryption** to *AES128* with *SHA1* authentication.

Set **2 - Encryption** to *3DES* with *SHA1* authentication.

Enable **Perfect Forward Secrecy (PFS)** and set **Keylife** to 3600 seconds.

## Assigning an IP to the VPN interface (optional)

If you wish to control the IP address that will be assigned to any traffic egressing over the IPsec interface, you can assign an IP to the interface.

Go to **System > Network > Interfaces**. Expand your Internet-facing interface and edit the VPN interface.

Assign the **IP** and **Remote IP** addresses. These addresses should not be related to the IPs used for the internal network or the Internet-facing interface.

NameAndroidVPN

CommentsWrite a comment...0/255

Phase 1AndroidVPN

Advanced...

P2 Proposal

1- Encryption: AES128 Authentication: SHA1

2- Encryption: 3DES Authentication: SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy (PFS).

DH Group 1 2 5 14

Keylife:Seconds3600(Seconds)5120(KBytes)

Autokey Keep Alive☐ Enable

Auto-negotiate☐ Enable

DHCP-IPsec☐ Enable








Name	AndroidVPN
Type	Tunnel Interface
Interface	wan1
Addressing modeManual	
IP	10.10.80.1
Remote IP	172.16.2.5
IPv6 Address	::/0

## Creating a security policy for access to the internal network and the Internet

Go to **Policy > Policy > Policy**.

Create a security policy allowing remote Android users to access the internal network.

The source interface is the AndroidVPN interface.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	AndroidVPN 
Source Address	all 
Outgoing Interface	lan 
Destination Address	Local LAN 
Schedule	always 
Service	ALL 
Action	ACCEPT 
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address <input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool <input type="text" value="Click to add..."/>	
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	

## Configuring VPN using FortiClient on the Android device

On your Android device, open FortiClient and select **Add IPsec VPN**.

Enter an account name for the IPsec account and press **OK**.

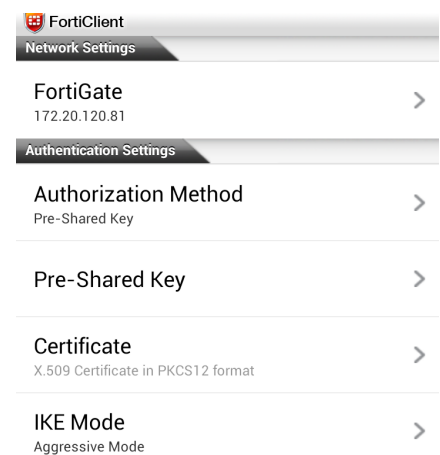
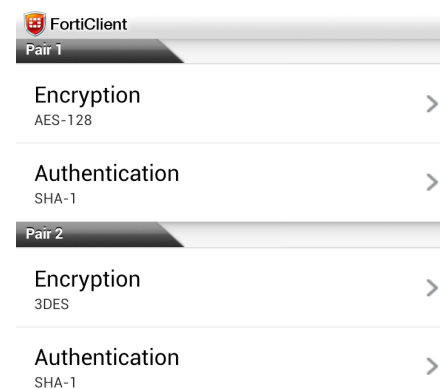
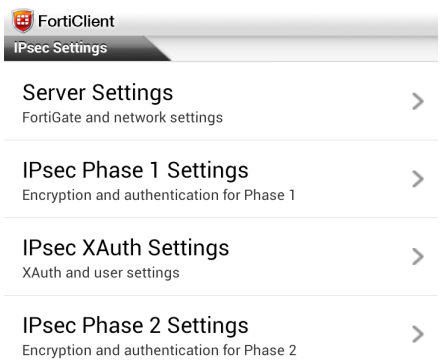


The IPsec settings menu appears.

Begin by configuring the Phase 1 and Phase 2 encryption and authentication settings to match those of the FortiGate

Under **Server Settings > Network Settings**, enter the address of the FortiGate interface that is connected to the Internet.

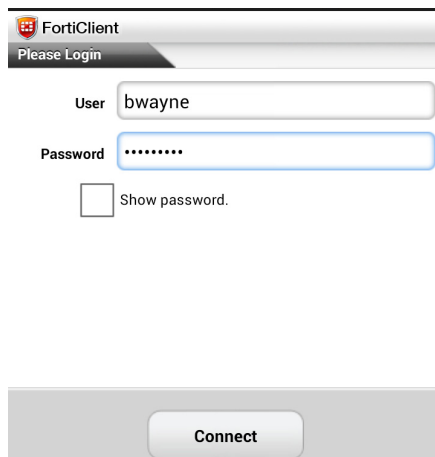
Under **Server Settings > Authentication Settings**, enter the pre-shared key that you created during Phase 1 configuration on the FortiGate.



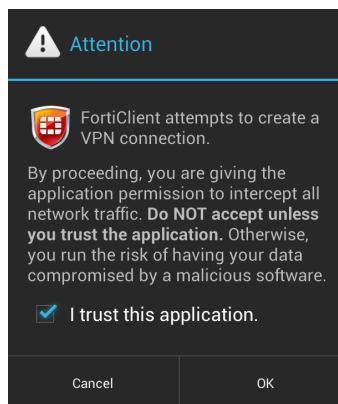
## Results

In FortiClient, access the newly created VPN and enter the assigned username and password, then press **Connect**.

As the FortiClient attempts to connect to the VPN, a warning message prompts you to trust the application.



The image shows the FortiClient login window. At the top, there is a title bar with the FortiClient logo and the text "Please Login". Below this, there are two input fields: "User" with the text "bwayne" and "Password" with a masked password "\*\*\*\*\*". Below the password field, there is a checkbox labeled "Show password." which is currently unchecked. At the bottom of the window, there is a large "Connect" button.





Once the FortiClient connects to the VPN, a connection status window indicates the traffic flow and duration of the connection.

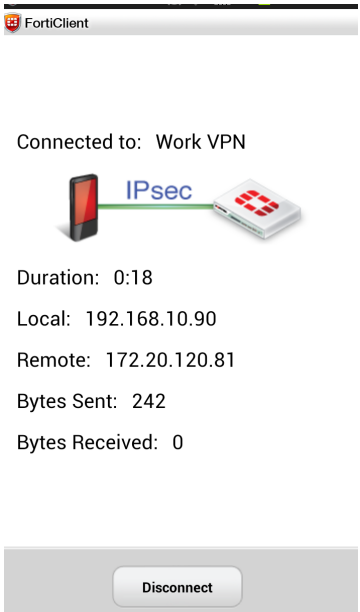
If there are problems connecting, check the event log on the FortiGate unit by going to **Log & Report > Log Access > Event Log**. The logs will show if the connection was successful. You can also use the following command to get more details about where the connection attempt failed:

```
diag debug application ike -1
```

The output can indicate something as simple as a pre-shared key mismatch, caused by the Android user entering the password incorrectly.

To verify that the tunnel has come up, go to **VPN > Monitor > IPsec Monitor**.

The AndroidVPN tunnel should appear in the list.



Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source
AndroidVPN_0	Dialup	172.20.120.126	64916	bwayne	3506	0.0.0.0-255.255.255
Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime		
192.168.10.90-192.168.10.90	Bring Down	288 B	0 B	83 seconds		

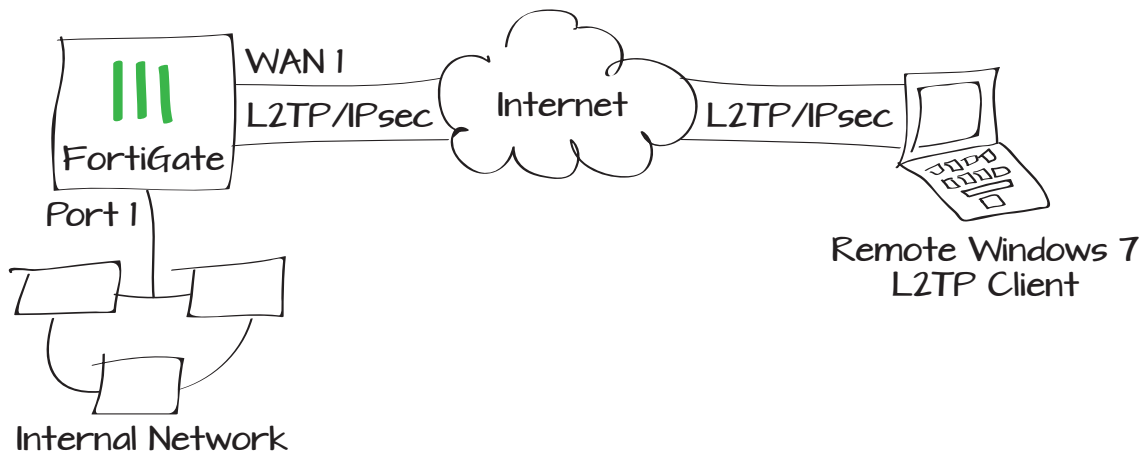
# Configuring a FortiGate unit as an L2TP/IPsec server

The FortiGate implementation of L2TP enables a remote dialup client to establish an L2TP/IPsec tunnel with the FortiGate unit directly. Creating an L2TP/IPsec tunnel allows remote users to connect to a private computer network in order to securely access their resources. For the tunnel to work you must configure a remote client to connect using an L2TP/IPsec VPN connection. This recipe is designed to work with a remote Windows 7 L2TP client.



The FortiGate unit must be operating in NAT/Route mode and have a static public IP address.

1. Creating an L2TP user and user group
2. Enabling L2TP on the FortiGate
3. Configuring the L2TP/IPsec phases
4. Creating a security policy for access to the internal network and the Internet
5. Configuring a remote Windows 7 L2TP client
6. Results



## Creating an L2TP user and user group

Go to **User & Device > User > User Definition**.

Create a new L2TP user for each remote client.

Go to **User & Device > User > User Groups**.

Create a user group for L2TP users and add the users you created.

## Enabling L2TP on the FortiGate

Enable L2TP on the FortiGate and assign an IP range for L2TP users.

Go to **System > Dashboard > Status > CLI Console** and enter the CLI commands shown here.

The **sip** indicates the starting IP in the IP range. The **eip** indicates the ending IP in the IP range.

User Name

☐ Disable

☒ Password

☐ Match user on LDAP server

☐ Match user on RADIUS server

☐ Match user on TACACS+ server

Name

Type ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest

Single Sign-On (RSSO)

Members

Remote authentication servers

Remote Server	Group Name
No matching entries found	

OK Cancel

```
config vpn L2TP
  set sip 192.168.10.1
  set eip 192.168.10.101
  set status enable
  set usrgrp L2TP_users
end
```

# Configuring the L2TP/IPsec phases

On the FortiGate, go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.

Enable all of the **DH Groups** and disable **Dead Peer Detection**.

When you are finished with Phase 1, select **Create Phase 2**. Name it appropriately and set it to use the new L2TP Phase 1.

Expand the **Advanced** options and specify a suitable **Keylife**. For example, **3600** seconds and **250000** KBytes.

Name

L2TP

Comments

Write a comment... 0/255

Remote Gateway

Dialup User

Local Interface

wan1

Mode

Aggressive

Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

Accept any peer ID

Accept this peer ID

Accept peer ID in dialup group

Android\_Users

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1 2 5 14

Keylife

28800 (120-172800 seconds)

Local ID

(optional)

XAUTH

Disable

Enable as Client

Enable as Server

NAT Traversal

Enable

Keepalive Frequency

10 (10-900 seconds)

Dead Peer Detection

Enable

Name

L2TP\_P2

Comments

Write a comment... 0/255

Phase 1

L2TP

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group

1 2 5 14

Keylife:

Both

3600 (Seconds)

250000 (KBytes)

Go to **System > Dashboard > Status > CLI Console**. In the **CLI Console** widget, edit the Phase 2 encapsulation mode using the CLI commands shown here.

```
config vpn ipsec phase2
    edit L2TP_P2
        set encapsulation transport-mode
    end
```

# Creating a security policy for access to the internal network and the Internet

To ensure that policy-based IPsec VPN is enabled, go to **System > Config > Features**, set **Policy-based IPsec VPN** to be turned on, and click **Apply**.



Go to **Policy > Policy > Policy**.

Create an **IPsec VPN** security policy allowing remote L2TP users to access the internal network.



Since L2TP is encapsulated on the data link layer, only one policy is required for incoming requests to WAN1.

Set both the **Local Interface** and the **Outgoing VPN Interface** to **wan1**.

Set both the **Local Protected Subnet** and the **Remote Protected Subnet** to **all**.

Next to **VPN Tunnel**, select **L2TP** and **Allow traffic to be initiated from the remote site**.

Policy Type	<input type="radio"/> Firewall <input checked="" type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> IPsec <input type="radio"/> SSL-VPN
Local Interface	wan1
Local Protected Subnet	all
Outgoing VPN Interface	wan1
Remote Protected Subnet	all
Schedule	always
Service	ALL
<b>Logging Options</b>	
<input type="radio"/> No Log	
<input type="radio"/> Log Security Events	
<input checked="" type="radio"/> Log all Sessions	
<b>VPN Tunnel</b>	
<input type="radio"/> Create New <input checked="" type="radio"/> Use Existing	
VPN Tunnel	L2TP
<input checked="" type="checkbox"/> Allow traffic to be initiated from the remote site	

## Configuring a remote Windows 7 L2TP client

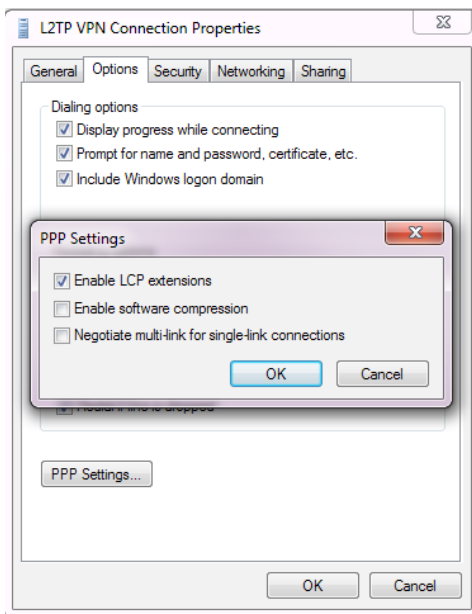
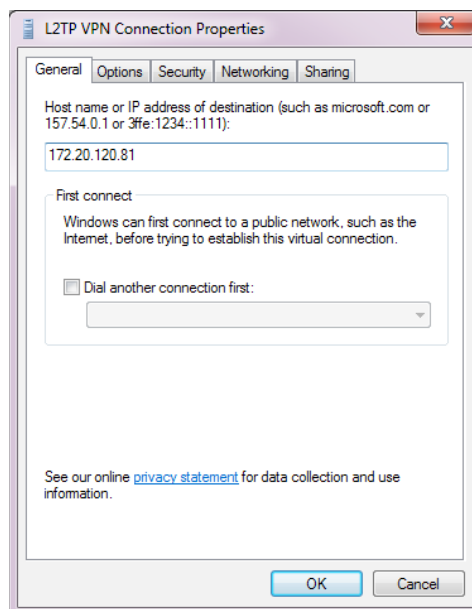
To connect to the FortiGate using L2TP, the remote client must be configured for L2TP/IPsec. The following configuration was tested on a PC running Windows 7.

On the Windows PC, create a new VPN connection.

Right-click on the new connection and select **Properties**, then modify the connection with the settings shown.

The **Host name** is the wan1 interface of the FortiGate unit that is acting as the L2TP/IPsec server.

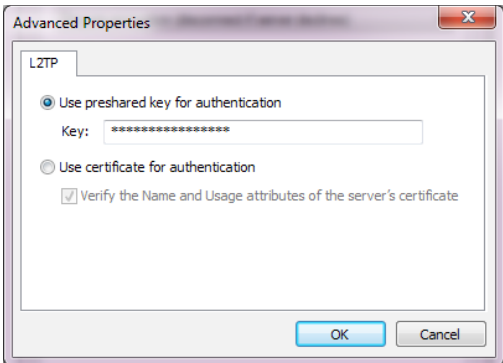
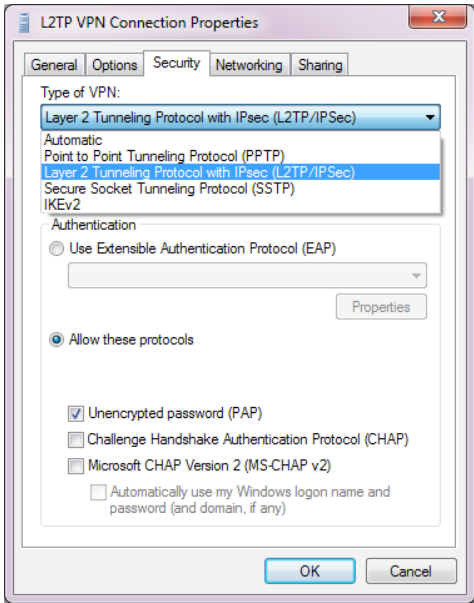
Under the **Options** tab, enable **LCP extensions**.



Under the **Security** tab, set the **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

Ensure that you allow only **Unencrypted password (PAP)** protocol. Disable other protocols.

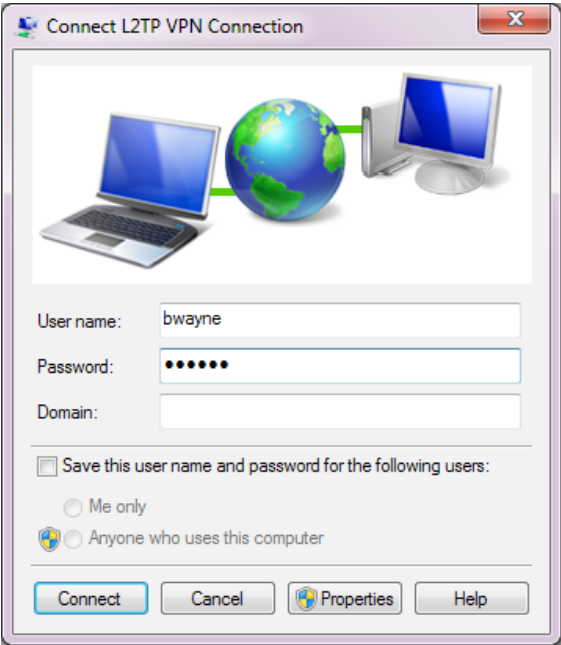
Click **Advanced Settings** and enter the pre-shared key you created in the Phase 1 configuration on the FortiGate.



# Results

On the remote user's PC, connect to the Internet using the L2TP/IPsec connection you created.

Enter the L2TP user's credentials and click **Connect**.



Verify the connection in the GUI by navigating to **VPN > Monitor > IPsec Monitor**.

You can view more detailed information in the event log. Go to **Log & Report > Event Log > VPN**.



Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID Source
L2TP_0	Dialup	172.20.120.222	0		3584	172.20.120.81-172.20.120.81
Proxy ID Destination	Status	Incoming Data	Outgoing Data	Uptime		
172.20.120.222-172.20.120.222	<a href="#">Bring Down</a>	552 B	0 B	3 seconds		

Level	Action	Status	
	negotiate	success	negotiate IPsec phase 2
	negotiate	success	progress IPsec phase 2
	tunnel-up		IPsec connection status change
	phase2-up		IPsec phase 2 status change
	install_sa		install IPsec SA
	negotiate	success	progress IPsec phase 2
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1
	negotiate	success	progress IPsec phase 1



Select an entry to view the connection details, including **IPSec Local IP**, **IPSec Remote IP**, **VPN Tunnel** type, **User**, and more.

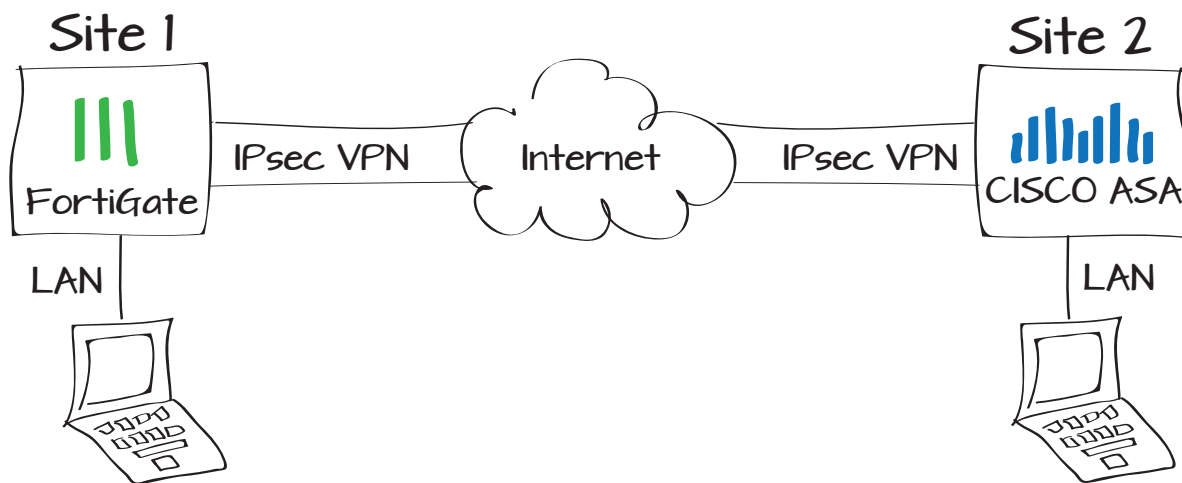
The **IPSec Remote IP** shown here should match the **Remote Gateway** shown under **VPN > Monitor > IPsec Monitor**.

Action	negotiate	Cookies	ba6132a63bde0998/b8f7fc6b07cdc7bb
Date/Time	13:13:15 (1380805995)	ESP Auth	HMAC_SHA1
ESP Transform	ESP_AES	Group	N/A
IPSec Local IP	172.20.120.81	IPSec Remote IP	172.20.120.222
Level	notice 	Local Port	500
Log ID	37122	Message	negotiate IPsec phase 2
Outgoing Interface	wan1	Remote Port	500
Role	responder	Status	success
Sub Type	vpn	Timestamp	Thu Oct 3 13:13:15 2013
User	 bwayne	VPN Tunnel	L2TP
Virtual Domain	root	XAUTH Group	N/A
XAUTH User	N/A		

# Configuring IPsec VPN with a FortiGate and a Cisco ASA

The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is behind a Cisco ASA. Using FortiOS 5.0 and Cisco ASDM 6.4, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied. The procedure assumes that both devices are configured with appropriate internal and external interfaces.

1. Configuring the Cisco device using the IPsec VPN Wizard
2. Configuring the FortiGate tunnel phases
3. Configuring the FortiGate policies
4. Configuring the static route in the FortiGate
5. Results



## Configuring the Cisco device using the IPsec VPN Wizard

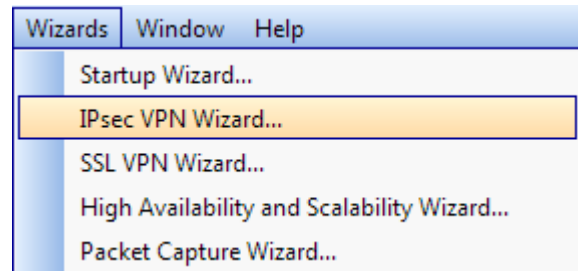
In the Cisco ASDM, under the **Wizard** menu, select **IPsec VPN Wizard**.

From the options that appear, select **Site-to-site**, with the **VPN Tunnel Interface** set to **outside**, then click **Next**.

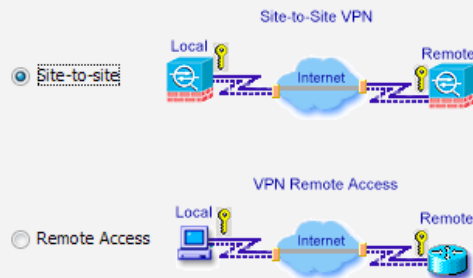
In the **Peer IP Address** field, enter the IP address of the FortiGate unit through which the SSL VPN traffic will flow.

Under **Authentication Method**, enter a secure **Pre-Shared Key**. You will use the same key when configuring the FortiGate tunnel phases. Choose something more secure than “Password”.

When you are satisfied, click **Next**.



VPN Tunnel Type:



VPN Tunnel Interface: **outside**

☒ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

Configure the IP address of the peer device, authentication method and the tunnel group for this site-to-site tunnel.

Peer IP Address: **172.20.120.81**

Authentication Method

☒ Pre-shared key

Pre-Shared Key: **Password**

☐ Certificate

Certificate Signing Algorithm: **rsa-sig**

Certificate Name:

The next steps in the IPsec VPN Wizard is to establish the tunnel phases 1 and 2.



The encryption settings established here must match the encryption settings configured later in the FortiGate.

Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

Set the **Diffie-Hellman Group** to **5**.

Configure Phase 1 with **AES-256 Encryption** and **SHA Authentication**.

Enable **PFS** and set the **Diffie-Hellman Group** to **2**.

Click **Next**.

Set the **Local Network** and **Remote Network**.

Click **Next** and review the configuration before you click **Finish**.

The tunnel configuration on the Cisco ASA is complete. Now you must configure the FortiGate with similar settings, except for the remote gateway.

Encryption: AES-256

Authentication: SHA

Diffie-Hellman Group: 5

Encryption: AES-256

Authentication: SHA

☒ Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 2

Local Networks: inside-network/24

Remote Networks: 172.20.120.81

You have created a Site-to-Site VPN tunnel with the following attributes:

VPN Tunnel Interface: outside  
Peer IP Address: 172.20.120.81  
IPsec authentication uses pre-shared key: Password  
Tunnel Group Name: 172.20.120.81  
IKE Policy Encryption / Authentication / Diffie-Hellman Group: AES-256 / SHA / Group 5  
IPsec ESP Encryption / ESP Authentication: AES-256 / SHA  
Perfect Forward Secrecy (PFS): enabled  
Diffie-Hellman Group: 2  
Traffic flow to be protected by this tunnel:  
(local) 192.168.1.0/24  
(remote) 172.20.120.81

# Configuring the FortiGate tunnel phases

In the FortiOS GUI, navigate to **VPN > IPsec > Auto Key (IKE)** and select **Create Phase 1**.

Name the tunnel, statically assign the **IP Address** of the remote gateway, and set the **Local Interface** to **wan1**.

Select **Preshared Key** for **Authentication Method** and enter the same preshared key you chose when configuring the Cisco IPsec VPN Wizard.

Configure this phase to match the encryption settings configured on the Cisco device and click **OK**.

Select **Create Phase 2**.

Identify Phase 1, which you just configured, and ensure that the encryption settings match the Phase 2 encryption settings configured on the Cisco device.

Optionally, under **Quick Mode Selector**, specify the **Source address** and **Destination address** at the endpoints of the tunnel.

NameSite2Site

CommentsWrite a comment...0/255

Remote GatewayStatic IP Address

IP Address172.20.120.222

Local Interfacewan1

Mode

Aggressive

Main (ID protection)

Authentication MethodPreshared Key

Pre-shared Key

Peer Options

Accept any peer ID

Enable IPsec Interface Mode

IKE Version

1

2

Mode Config

Local Gateway IP

Main Interface IP

Specify0.0.0.0

P1 Proposal

1 - EncryptionAES256AuthenticationSHA1

DH Group

1

2

5

14

Keylife28800(120-172800 seconds)

Local ID(optional)

NameSite2Site2

CommentsWrite a comment...0/255

Phase 1Site2Site

Advanced...

P2 Proposal

1- Encryption: AES256Authentication: SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group

1

2

5

14

Keylife:Seconds1800(Seconds)5120(KBytes)

Autokey Keep Alive

Enable

Auto-negotiate

Enable

Quick Mode Selector

Source address

Specify192.168.100.0/24

Select-----Address-----

Source port0

Destination address

Specify192.168.1.0/24

Select-----Address-----

Destination port0

Protocol0

# Configuring the FortiGate policies

Navigate to **Policy > Policy > Policy** and create firewall policies that allow inbound and outbound traffic over the tunnel.

In the first (outbound) policy, set the **Incoming Interface** to **lan** and set the **Source Address** to **all**.

Set the **Outgoing Interface** to the tunnel interface and set the **Destination Address** to **all**. Configure the **Schedule** and **Service** as desired.

Create the second (inbound) policy to allow traffic to flow in the opposite direction, and configure the **Schedule** and **Service** as desired.

# Configuring the static route in the FortiGate

Navigate to **Router > Static > Static Routes** and select **Create New**.

Create a static route with the **Destination IP/Mask** matching the address of the Cisco local network (by default, 192.168.1.0).

Under **Device**, select the site-to-site tunnel, and click **OK**.

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

lan

Source Address

all

Outgoing Interface

Site2Site

Destination Address

all

Schedule

always

Service

ALL

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

Site2Site

Source Address

all

Outgoing Interface

lan

Destination Address

all

Schedule

always

Service

ALL

Destination IP/Mask

192.168.1.0/255.255.255.0

Device

Site2Site

Distance

10

(1-255, Default=10)

Priority

0

(0-4294967295)

Comments

Write a comment...

0/255

# Results

The tunnel should now be active. On the FortiGate, verify that the tunnel is ‘up’ by navigating to **VPN > Monitor > IPsec Monitor**.

The IPsec Monitor table will indicate the source and destination addresses, and the status of the tunnel (up or down) and its uptime.

For more detailed tunnel information, go to **Log & Report > Event Log > VPN** and view the table.

Select the tunnel entry in the table to view the information in greater detail.

Name	Type	Remote Gateway	Remote Port	Username	Timeout	Proxy ID	Source
Site2Site	Static IP or Dynamic DNS	172.20.120.222	0		888	192.168.100.0/24	
Proxy ID	Destination	Status	Incoming Data	Outgoing Data	Uptime		
192.168.1.0/24		Bring Down	0 B	2169 B	2570 seconds		

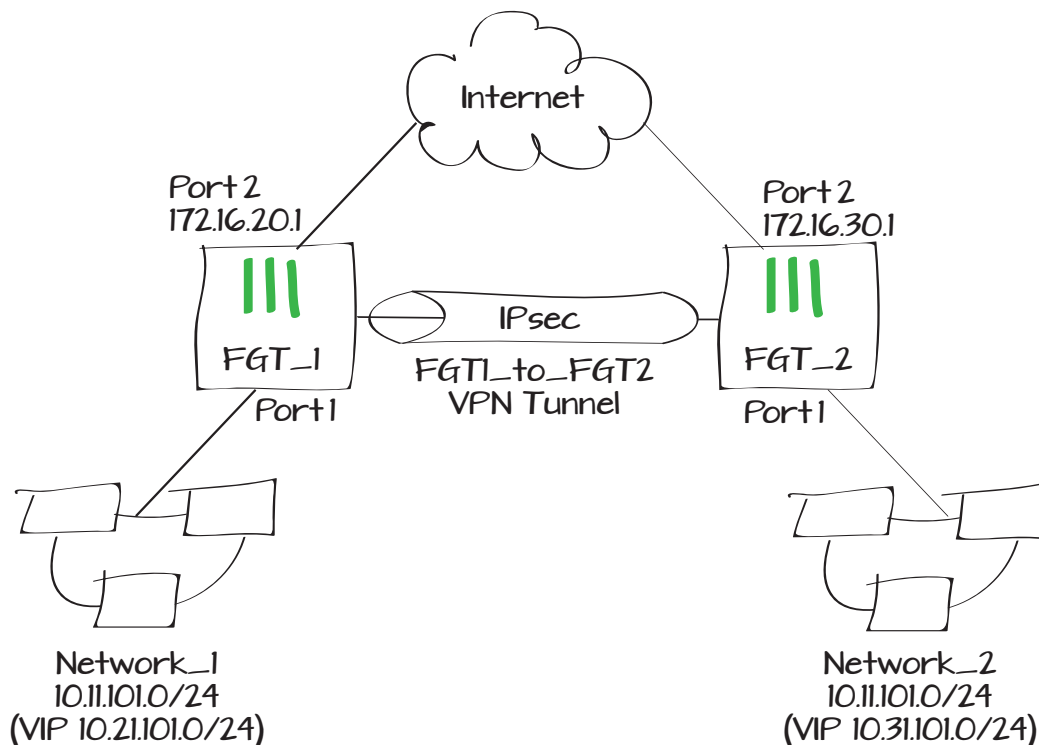
#	Date/Time	Level	Action	Status	Message	VPN Tunnel
1	14:38:17		negotiate	success	negotiate IPsec phase 2	Site2Site
2	14:38:17		negotiate	success	progress IPsec phase 2	Site2Site
3	14:38:17		install_sa		install IPsec SA	Site2Site
4	14:38:17		negotiate	success	progress IPsec phase 2	Site2Site
5	14:09:46		negotiate	success	negotiate IPsec phase 2	Site2Site
6	14:09:46		negotiate	success	progress IPsec phase 2	Site2Site
7	14:09:46		tunnel-up		IPsec connection status change	Site2Site
8	14:09:46		phase2-up		IPsec phase 2 status change	Site2Site
9	14:09:46		install_sa		install IPsec SA	Site2Site
10	14:09:46		negotiate	success	progress IPsec phase 2	Site2Site
11	14:09:46		negotiate	success	progress IPsec phase 1	Site2Site
12	14:09:46		negotiate	success	progress IPsec phase 1	Site2Site

Action	negotiate	Cookies	c2a44adda34edfff/a3945a75a39f2f2f
Date/Time	14:38:17 (1384353497)	ESP Auth	HMAC_SHA1
ESP Transform	ESP_AES	Group	N/A
IPsec Local IP	172.20.120.81	IPsec Remote IP	172.20.120.222
Level	notice	Local Port	500
Log ID	37122	Message	negotiate IPsec phase 2
Outgoing Interface	wan1	Remote Port	500
Role	responder	Status	success
Sub Type	vpn	Timestamp	Wed Nov 13 14:38:17 2013
User	N/A	VPN Tunnel	Site2Site
Virtual Domain	root	XAUTH Group	N/A
XAUTH User	N/A		

# Creating a VPN with overlapping subnets

This recipe describes how to construct a VPN connection between two networks with overlapping IP addresses in such a way that traffic will be directed to the correct address on the correct network, using Virtual IP addresses and static routes.

1. Creating VPN tunnels between the two FortiGate units
2. Adding the virtual IP range and address
3. Creating inbound and outbound security policies
4. Configuring static routes
5. Repeat the steps on FGT2
6. Results





# Creating VPN tunnels between the two FortiGates

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**, and set the **IP Address** to the address used by the Internet-facing interface of FGT\_2. Set the **Local Interface** to your Internet-facing interface, and enter a **Pre-shared Key**.

Then create the Phase 2, selecting your Phase 1 from the list.

# Adding the virtual IP range and address

Go to **Firewall Objects > Virtual IPs > Virtual IPs**.

You will need to create a Virtual IP range that will be used to redirect the traffic to the correct subnet. Give the VIP an appropriate name, and set the IPsec tunnel interface as the **External Interface**.

Set the **External IP Address** to a range in the subnet you'll be redirecting from (10.21.101.1-10.21.101.254) and the **Mapped IP address** to the internal network range (10.11.101.1-10.11.101.254).

Name	FGT1_to_FGT2
Comments	Write a comment... 0
Remote Gateway	Static IP Address
IP Address	172.16.30.1
Local Interface	wan1
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	Preshared Key
Pre-shared Key	.....

Name	To_FGT2_P2
Comments	Write a comment... 0/255
Phase 1	FGT1_to_FGT2

Name	VPN_VIP
Comments	Write a comment...
Color	[Change]
External Interface	FGT1_to_FGT2
Type	Static NAT
<input type="checkbox"/> Source Address Filter	
External IP Address/Range	10.21.101.1 - 10.21.101.254
Mapped IP Address/Range	10.11.101.1 - 10.11.101.254
<input type="checkbox"/> Port Forwarding	

Now go to **Firewall Objects > Address > Addresses**.

Create a new address, setting the **Type** to **IP Range**, and entering the VIP range of FGT2 (10.31.101.1-10.31.101.254).

## Creating inbound and outbound security policies

Go to **Policy > Policy > Policy**.

Create a firewall policy to handle outbound VPN traffic, with the network-facing interface as the **Incoming Interface**, and the IPsec interface as **Outgoing**. Set the **Destination Address** to the VIP Address Range. Enable NAT.

Create a second security policy to handle inbound VPN traffic, with the IPsec interface as the **Incoming Interface**, network-facing interface as **Outgoing**, and your VIP range as the **Destination Address**. Disable NAT.

Category

Name

Color

Type

Subnet / IP Range

Interface

Show in Address List

Address

IPv6 Address

Multicast Address

FGT2 Range

[Change]

IP Range

10.31.101.1-10.31.101.254

Any

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Firewall

VPN

Address

User Identity

Device Identity

port1 (Internal)

all

FGT1\_to\_FGT2

FGT2 Range

always

ALL

ACCEPT

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

Enable NAT

Firewall

VPN

Address

User Identity

Device Identity

FGT1\_to\_FGT2

FGT2 Range

port1 (Internal)

VPN\_VIP

always

ALL

ACCEPT

# Configuring static routes

Go to **Router > Static > Static Routes**.

Create a new Static Route, with the **Destination IP** as 10.31.101.0/24. For your **Device**, select your FGT1\_to\_FGT2 VPN interface. Set **Distance** to lower than the default of 10 to prioritize this route.

# Repeat these steps on FGT2

First, create the Phase 1 on FGT\_2, using FGT\_1's Internet-facing interface IP for the Phase 1 IP Address, and the FGT\_2's Internet-facing interface as **Local Interface**.

Create the Phase 2 for FGT\_2.

Destination IP/Mask	<input type="text" value="10.31.101.0/24"/>
Device	<input type="text" value="FGT1_to_FGT2"/>
Distance	<input type="text" value="5"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)

Name	<input type="text" value="FGT2_to_FGT1"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Remote Gateway	<input type="text" value="Static IP Address"/>
IP Address	<input type="text" value="172.16.20.1"/>
Local Interface	<input type="text" value="wan1"/>
Mode	<input type="radio"/> Aggressive <input checked="" type="radio"/> Main (ID protection)
Authentication Method	<input type="text" value="Preshared Key"/>
Pre-shared Key	<input type="text" value="....."/>

Name	<input type="text" value="To_FGT1_P2"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Phase 1	<input type="text" value="FGT2_to_FGT1"/>

Create the VIP Range, setting the IPsec tunnel interface as the **External Interface**, the **External IP Address** to the intended local VIP range (10.31.101.1-10.31.101.254) and the **Mapped IP Address** to the internal network range (10.11.101.1-10.11.101.254).

Create the address range, setting the **Type** to **IP Range**, and entering the VIP range of FGT1 (10.21.101.1-10.21.101.254).

Create the two firewall policies to handle outbound and inbound VPN traffic.

For the outbound policy, select your internal-network-facing port as the **Incoming Interface**, and the IPsec interface as **Outgoing**. Set the **Destination Address** to the VIP Address Range. Enable NAT.

For the inbound, set the IPsec interface as the **Incoming Interface**, internal port as **Outgoing**, and your VIP range as the **Destination Address**. Disable NAT.

Name

VPN\_VIP\_2

Comments

Write a comment...

Color

[Change]

External Interface

FGT2\_to\_FGT1

Type

Static NAT

☐ Source Address Filter

External IP Address/Range

10.31.101.1 - 10.31.101.254

Mapped IP Address/Range

10.11.101.1 - 10.11.101.254

☐ Port Forwarding

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT1 Range

Color

[Change]

Type

IP Range

Subnet / IP Range

10.21.101.1-10.21.101.254

Interface

Any

Show in Address List

☒

Incoming Interface

port1 (Internal)

Source Address

all

Outgoing Interface

FGT2\_to\_FGT1

Destination Address

FGT1 Range

Schedule

always

Service

ALL

Action

☒ Enable NAT

 ACCEPT

Incoming Interface

FGT2\_to\_FGT1

Source Address

FGT1 Range

Outgoing Interface

port1 (Internal)

Destination Address

VPN\_VIP\_2

Schedule

always

Service

ALL

Action

☐ Enable NAT

 ACCEPT

Then create the Static Route, with the **Destination IP** as 10.21.101.0/24. For your **Device**, select your VPN interface.

Set the Distance lower than 10.

# Results

On a FortiGate unit, you can go to **VPN > Monitor > IPsec Monitor** to see the status of the VPN tunnel.

Connect to the VPN, using a network device in Network\_1. Access the address 10.31.101.50, and your session will be redirected to Network\_2's 10.11.101.50.

Then, from a VPN-connected device in Network\_2, visit 10.21.101.50, and you will access Network\_1's 10.11.101.50.

Go to **Log & Report > Traffic Log > Forward Traffic** and filter the **Src Interface** column with the VPN Interface name to see incoming VPN traffic and the **Dst Interface** column to see outgoing.

Destination IP/Mask

Device

Distance  (1-255, Default=10)

Priority  (0-4294967295)

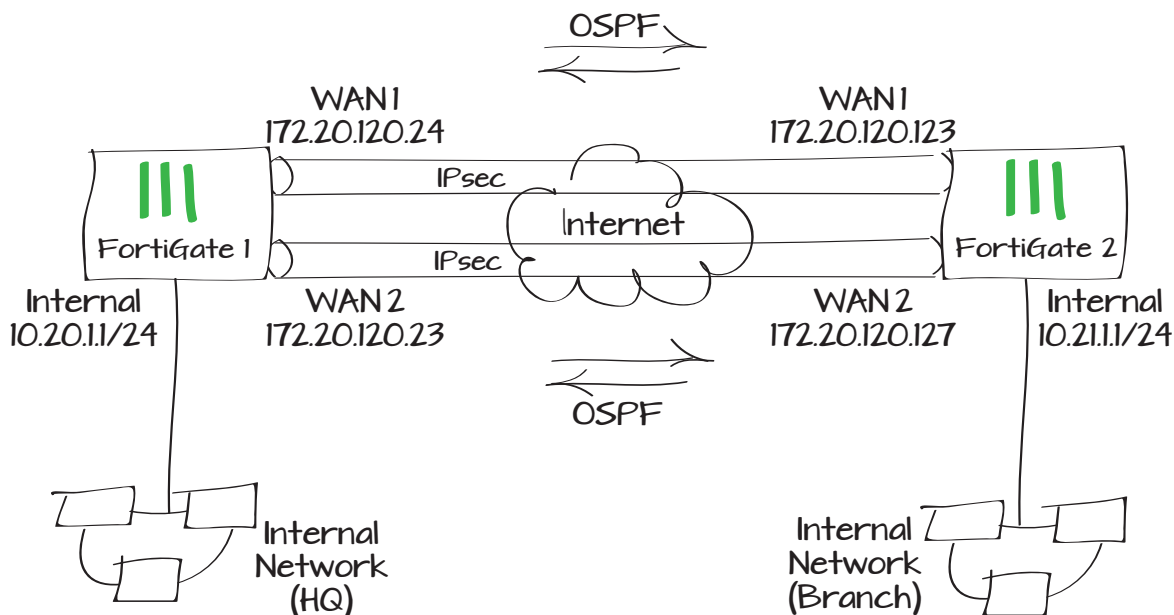
Name	Type	Status	Remote Gateway
FGT1_to_FGT2	Static IP or Dynamic DNS	Bring Down	172.16.30.1

#	Date/Time	Src	Dst	Sent / Received	Src Interface	Dst Interface
1	13:08:57	10.11.101.50	10.31.101.50	2.05 KB / 2.05 KB	port1	FGT1_to_FGT2
2	12:51:20	10.11.101.50	10.31.101.50	14.77 KB / 14.77 KB	port1	FGT1_to_FGT2
3	12:46:53	10.11.101.50	10.31.101.50	6.50 KB / 6.33 KB	port1	FGT1_to_FGT2

# Using redundant OSPF routing over IPsec VPN

This example sets up redundant secure communication between two remote networks using an Open Shortest Path First (OSPF) VPN connection. In this example, the HQ FortiGate unit will be called FortiGate 1 and the Branch FortiGate unit will be called FortiGate 2.

1. Creating redundant IPsec tunnels on FortiGate 1
2. Configuring IP addresses and OSPF on FortiGate 1
3. Configuring firewall addresses on FortiGate 1
4. Configuring security policies on FortiGate 1
5. Creating redundant IPsec tunnels for FortiGate 2
6. Configuring IP addresses and OSPF on FortiGate 2
7. Configuring firewall addresses on FortiGate 2
8. Configuring security policies on FortiGate 2
9. Results



# Creating redundant IPsec tunnels on FortiGate 1

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1** and create the primary tunnel. Set **IP Address** to FortiGate 2's wan1 IP, **Local Interface** to **wan1** (the primary Internet-facing interface) and enter a **Pre-shared Key**.

Select **Create Phase 2**. Set it to use the new Phase 1.

Name

To-TGT2\_Primary

Comments

Primary IPsec vpn to FortiGate2 31/255

Remote Gateway

Static IP Address

IP Address

172.20.120.123

Local Interface

wan1

Mode

Aggressive

Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

Accept any peer ID

IKE Version

1

2

Mode Config

IPv6 Version

Local Gateway IP

Main Interface IP

Specify

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1

2

5

14

Keylife

28800 (120-172800 seconds)

Local ID

(optional)

XAUTH

Disable

Enable as Client

Enable as Server

NAT Traversal

Enable

Keepalive Frequency

10 (10-900 seconds)

Dead Peer Detection

Enable

Name

P2\_To\_FGT2\_Primary

Comments

Phase 2 7/255

Phase 1

To\_FGT2\_Primary

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

Enable replay detection

Enable perfect forward secrecy (PFS)

DH Group

1

2

5

14

15

16

17

18

19

20

21

Keylife:

Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive

Enable

Quick Mode Selector

Source address

Specify

0.0.0.0/0

Select

-----Address-----

Source port

0

Destination address

Specify

0.0.0.0/0

Select

-----Address-----

Destination port

0

Protocol

0

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1** and create the secondary tunnel. Set **IP Address** to use FortiGate 2's wan2 IP, **Local Interface** to **wan2** (the secondary Internet-facing interface) and enter the **Pre-shared Key**.

Name

To-TGT2\_Second

Comments

Secondary IPsec vpn to FortiGate2 33/255

Remote Gateway

Static IP Address

IP Address

172.20.120.127

Local Interface

wan2

Mode

Aggressive

Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

Accept any peer ID

IKE Version

1

2

Mode Config

IPv6 Version

Local Gateway IP

Main Interface IP

Specify

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1

2

5

14

Keylife

28800 (120-172800 seconds)

Local ID

(optional)

XAUTH

Disable

Enable as Client

Enable as Server

NAT Traversal

Enable

Keepalive Frequency

10 (10-900 seconds)

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 2**. Set it to use the new Phase 1

Name

P2\_To\_FGT2\_Second

Comments

Write a comment... 0/255

Phase 1

To\_FGT2\_Second

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

Enable replay detection

Enable perfect forward secrecy (PFS).

DH Group

1

2

5

14

Keylife:

Seconds

1800 (Seconds)

4608000 (KBytes)

Autokey Keep Alive

Enable

Auto-negotiate

Enable

Quick Mode Selector

Source address

Specify

0.0.0.0/0

Select

-----Address-----

Source port

0

Destination address

Specify

0.0.0.0/0

Select

-----Address-----



# Configuring IP addresses and OSPF on FortiGate 1

Go to **System > Network > Interfaces**.

Select the arrow for **wan1** to expand the list. Edit the primary tunnel interface and create IP addresses.

Select the arrow for wan2 to expand the list. Edit the secondary tunnel interface and create IP addresses.

Go to **Router > Dynamic > OSPF**.

Enter the **Router ID** for FortiGate 1.

Select **Create New** in the **Area** section.

Add the backbone area of 0.0.0.0.

Select **Create New** in the **Networks** section.

Create the networks and select Area 0.0.0.0 for each one.

Name

To\_FGT2\_Primary

Type

Tunnel Interface

Interface

wan1

Addressing mode

Manual

IP

10.1.1.1

Remote IP

10.1.1.2

IPv6 Address

::/0

Name

To\_FGT2\_Second

Type

Tunnel Interface

Interface

wan2

Addressing mode

Manual

IP

10.2.1.1

Remote IP

10.2.1.2

IPv6 Address

::/0

Router ID

1.1.1.1

Advanced Options

(Default, Redistribution)

	Area	Type	Authentication
<input type="checkbox"/>	0.0.0.0	Regular	None

	Network	Area
<input type="checkbox"/>	10.1.1.1/255.255.255.255	0.0.0.0
<input type="checkbox"/>	10.2.1.1/255.255.255.255	0.0.0.0
<input type="checkbox"/>	10.20.1.0/255.255.255.0	0.0.0.0




Select **Create New** in the **Interfaces** section.

Create primary and secondary tunnel interfaces. Set a **Cost** of 10 for the primary interface and 100 for the secondary interface.

## Configuring firewall addresses on FortiGate 1

Go to **Firewall Objects > Address > Addresses**.

Edit the subnets behind FortiGate 1 and FortiGate 2.

	Name	Interface	Cost	IP	Authenticat
	Primary_Tunnel	To_FGT2_Primary	10	0.0.0.0	None
	Secondary_Tunnel	To_FGT2_Second	100	0.0.0.0	None


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT1\_LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

10.20.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

LAN behind FortiGate1

 21/255


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT2\_LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

10.21.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

LAN behind FortiGate2

 21/255

Edit the primary and secondary interfaces of FortiGate 2.

# Configuring security policies on FortiGate 1

Go to **Policy > Policy > Policy**.

Create the four security policies required for both FortiGate 1’s primary and secondary interfaces to connect to FortiGate 2’s primary and secondary interfaces.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT2\_Primary\_Int

Color

[Change]

Type

Subnet

Subnet / IP Range

10.1.1.2

Interface

Any

Show in Address List

☒

Comments

IP of Primary IPsec interface in FortiGate2 43/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT2\_Secondary\_Int

Color

[Change]

Type

Subnet

Subnet / IP Range

10.2.1.2

Interface

Any

Show in Address List

☒

Comments

IP of Secondary IPsec interface in FortiGate2 45/255

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

FGT1\_LAN

Outgoing Interface

To\_FGT2\_Primary

Destination Address

FGT2\_LAN

Schedule

always

Service

any

Action

ACCEPT

☐ Enable NAT

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	To_FGT2_Primary
Source Address	<div>FGT2_LAN X +</div> <div>FGT2_Primary_Int X</div>
Outgoing Interface	internal
Destination Address	FGT1_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	internal
Source Address	FGT1_LAN +
Outgoing Interface	To_FGT2_Second
Destination Address	FGT2_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	To_FGT2_Second
Source Address	<div>FGT2_LAN X +</div> <div>FGT2_Secondary_Int X</div>
Outgoing Interface	internal
Destination Address	FGT1_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

# Creating redundant IPsec tunnels on FortiGate 2

Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1** and create the primary tunnel. Set **IP Address** to FortiGate 1's wan1 IP, **Local Interface** to **wan1** (the primary Internet-facing interface) and enter a **Pre-shared Key**.

Select **Create Phase 2**. Set it to use the new Phase 1.

Name

To\_FGT1\_Primary

Comments

Primary IPsec vpn to FortiGate1 31/255

Remote Gateway

Static IP Address

IP Address

172.20.120.24

Local Interface

wan1

Mode

☐ Aggressive

☒ Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

.....

Peer Options

☒ Accept any peer ID

IKE Version

☒ 1

☐ 2

Mode Config

☐

Local Gateway IP

☒ Main Interface IP

☐ Specify 0.0.0.0

P1 Proposal

1 - Encryption 3DES Authentication SHA1

2 - Encryption AES128 Authentication SHA1

DH Group

☐ 1

☐ 2

☒ 5

☐ 14

Keylife

28800 (120-172800 seconds)

Local ID

(optional)

XAUTH

☒ Disable

☐ Enable as Client

☐ Enable as Server

NAT Traversal

☒ Enable

Keepalive Frequency

10 (10-900 seconds)

Dead Peer Detection

☒ Enable

Name

P2\_To\_FGT1\_Primary

Comments

Phase2 6/255

Phase 1

To\_FGT1\_Primary

Advanced...

P2 Proposal

1- Encryption: 3DES Authentication: SHA1

2- Encryption: AES128 Authentication: SHA1

☒ Enable replay detection

☒ Enable perfect forward secrecy (PFS).

DH Group

☒ 1

☐ 2

☒ 5

☐ 14

☐ 15

☐ 16

☐ 17

☐ 18

☐ 19

☐ 20

☐ 21

Keylife:

Seconds 1800 (Seconds) 5120 (KBytes)

Autokey Keep Alive

☐ Enable

Quick Mode Selector

Source address 

☐ Specify 0.0.0.0/0

☐ Select -----Address-----

Source port 0

Destination address 

☐ Specify 0.0.0.0/0

☐ Select -----Address-----

Destination port 0

Protocol 0

Select **Create Phase 1** and create the secondary tunnel. Set **IP Address** to use FortiGate 2's IP, **Local Interface** to **wan2** (the secondary Internet-facing interface) and enter the **Pre-shared Key**.

Name

To\_FGT1\_Second

Comments

Secondary IPsec vpn to FortiGate1

33/255

Remote Gateway

Static IP Address

IP Address

172.20.120.23

Local Interface

wan2

Mode

Aggressive

Main (ID protection)

Authentication Method

Preshared Key

Pre-shared Key

Peer Options

Accept any peer ID

IKE Version

1

2

Mode Config

IPv6 Version

Local Gateway IP

Main Interface IP

Specify

P1 Proposal

1 - Encryption

3DES

Authentication

SHA1

2 - Encryption

AES128

Authentication

SHA1

DH Group

1

2

5

14

Keylife

28800

(120-172800 seconds)

Local ID

(optional)

XAUTH

Disable

Enable as Client

Enable as Server

NAT Traversal

Enable

Keepalive Frequency

10

(10-900 seconds)

Dead Peer Detection

Enable

Select **Create Phase 2**. Set it to use the new Phase 1.

Name

P2\_To\_FGT1\_Second

Comments

Phase2

6/255

Phase 1

To\_FGT1\_Second

Advanced...

P2 Proposal

1- Encryption

3DES

Authentication

SHA1

2- Encryption

AES128

Authentication

SHA1

Enable replay detection

Enable perfect forward secrecy (PFS)

DH Group

1

2

5

14

15

16

17

18

19

20

21

Keylife:

Seconds

1800

(Seconds)

5120

(KBytes)

Autokey Keep Alive

Enable

Quick Mode Selector

Source address

Specify

0.0.0.0/0

Select

-----Address-----

Source port

0

Destination address

Specify

0.0.0.0/0

Select

-----Address-----

Destination port

0

Protocol

0

406

The FortiGate Cookbook 5.0.7

# Configuring IP addresses and OSPF on FortiGate 2

Go to **System > Network > Interfaces**.

Select the arrow for **wan1** to expand the list. Edit the primary tunnel interface and create IP addresses.

Select the arrow for **wan2** to expand the list. Edit the secondary tunnel interface and create IP addresses.

Go to **Router > Dynamic > OSPF**.

Enter the **Router ID** for FortiGate 2.

Select **Create New** in the **Area** section.

Add the backbone area of 0.0.0.0.

Select **Create New** in the **Networks** section.

Create the networks and select Area 0.0.0.0 for each one.

Name	To_FGT1_Primary
Type	Tunnel Interface
Interface	wan1

---

Addressing mode	Manual
IP	<input type="text" value="10.1.1.2"/>
Remote IP	<input type="text" value="10.1.1.1"/>
IPv6 Address	<input "::0"="" type="text" value=""/>

Name	To_FGT1_Second
Type	Tunnel Interface
Interface	wan2

---

Addressing mode	Manual
IP	<input type="text" value="10.2.1.2"/>
Remote IP	<input type="text" value="10.2.1.1"/>
IPv6 Address	<input "::0"="" type="text" value=""/>

**Router ID**

▶ **Advanced Options**(Default, Redistribution)

<input type="checkbox"/>	Area	Type	Authentication
<input type="checkbox"/>	0.0.0.0	Regular	None

<input type="checkbox"/>	Network	Area
<input type="checkbox"/>	10.1.1.2/255.255.255.255	0.0.0.0
<input type="checkbox"/>	10.2.1.2/255.255.255.255	0.0.0.0
<input type="checkbox"/>	10.21.1.0/255.255.255.0	0.0.0.0




Select **Create New** in the **Interfaces** section.

Create primary and secondary tunnel interfaces. Set a **Cost** of 10 for the primary interface and 100 for the secondary interface.

## Configuring firewall addresses on FortiGate 2

Go to **Firewall Objects > Address > Addresses**.

Edit the subnets behind FortiGate 1 and FortiGate 2.

	Name	Interface	Cost	IP	Authentication
	Primary_Tunnel	To_FGT1_Primary	10	0.0.0.0	None
	Secondary_Tunnel	To_FGT1_Second	100	0.0.0.0	None


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT1\_LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

10.20.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

LAN behind FGT1

 15/255


Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT2\_LAN

Color

 [Change]

Type

Subnet

Subnet / IP Range

10.21.1.0/255.255.255.0

Interface

Any

Show in Address List

☒

Comments

LAN behind FGT2

 15/255



Edit the primary and secondary interfaces of FortiGate 1.

# Configuring security policies on FortiGate 2

Go to **Policy > Policy > Policy**.

Create the four security policies required for both FortiGate 2's primary and secondary interfaces to connect to FortiGate 1's primary and secondary interfaces.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT1\_Primary\_Int

Color

[Change]

Type

Subnet

Subnet / IP Range

10.1.1.1

Interface

Any

Show in Address List

☒

Comments

IP of Primary IPSec Interface in FGT1 37/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FGT1\_Secondary\_Int

Color

[Change]

Type

Subnet

Subnet / IP Range

10.2.1.1

Interface

Any

Show in Address List

☒

Comments

IP of Secondary IPsec Interface in FG1 38/255

Policy Type

☒ Firewall ☐ VPN

Policy Subtype

☒ Address ☐ User Identity ☐ Device Identity

Incoming Interface

internal

Source Address

FGT2\_LAN +

Outgoing Interface

To\_FGT1\_Primary

Destination Address

FGT1\_LAN +

Schedule

always

Service

any +

Action

☒ ACCEPT

☐ Enable NAT

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	To_FGT1_Primary
Source Address	FGT1_LAN X + FGT1_Primary_Int X
Outgoing Interface	internal
Destination Address	FGT2_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	internal
Source Address	FGT2_LAN +
Outgoing Interface	To_FGT1_Second
Destination Address	FGT1_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	To_FGT1_Second
Source Address	FGT1_LAN X + FGT1_Secondary_Int X
Outgoing Interface	internal
Destination Address	FGT2_LAN +
Schedule	always
Service	any +
Action	✓ ACCEPT
<input type="checkbox"/> Enable NAT	

# Results

Go to **VPN > Monitor > IPsec Monitor** to verify the statuses of both the primary and secondary IPsec VPN tunnels on FortiGate 1 and FortiGate 2.

Go to **Router > Monitor > Routing. Monitor** to verify the routing table on FortiGate 1 and FortiGate 2. Type OSPF for the **Type** and select **Apply Filter** to verify the OSPF route.

Verify that traffic flows via the primary tunnel.

From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a traceroute to a PC2 set to IP address 10.21.1.00 behind FortiGate 2 and vice versa.

From PC1, you should see that the traffic goes through 10.1.1.2 which is the primary tunnel interface IP set on FortiGate 2.

From PC2, you should see the traffic goes through 10.1.1.1 which is the primary tunnel interface IP set on FortiGate 1.

The VPN network between the two OSPF networks uses the primary VPN connection. Disconnect the wan1 interface and

Name	Type	Remote Gateway	Remot
To_FGT1_Primary	Static IP or Dynamic DNS	172.20.120.24	0
To_FGT1_Second	Static IP or Dynamic DNS	172.20.120.23	0

Name	Type	Remote Gateway	Remot
To_FGT2_Primary	Static IP or Dynamic DNS	172.20.120.123	0
To_FGT2_Second	Static IP or Dynamic DNS	172.20.120.127	0

IP Version	Type	Subtype	Network	Gateway	Interface
4	OSPF		10.21.1.0/24	10.1.1.2	To_FGT2_Pri

IP Version	Type	Subtype	Network	Gateway	Interface
4	OSPF		10.20.1.0/24	10.1.1.1	To_FGT1_Primar

```
C:\>tracert 10.21.1.100

Tracing route to TELBAR-PC [10.21.1.100]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  10.20.1.1
  2  <1 ms  <1 ms  <1 ms  10.1.1.2
  3  1 ms   <1 ms  <1 ms  TELBAR-PC [10.21.1.100]

Trace complete.
```

```
C:\>tracert 10.20.1.100

Tracing route to TAHER_THINK [10.20.1.100]
over a maximum of 30 hops:
  1  <1 ms  <1 ms  <1 ms  10.21.1.1
  2  <1 ms  <1 ms  <1 ms  10.1.1.1
  3  1 ms   <1 ms  <1 ms  TAHER_THINK [10.20.1.100]

Trace complete.
```

confirm that the secondary tunnel will be used automatically to maintain a secure connection.

Verify the IPsec VPN tunnel statuses on FortiGate 1 and FortiGate 2. Both FortiGates should show that primary tunnel is DOWN and secondary tunnel is UP.

Go to **VPN > Monitor > IPsec Monitor** to verify the status.

Verify the routing table on FortiGate 1 and FortiGate 2.

The secondary OSPF route (with cost = 100) appears on both FortiGate units.

Go to **Router > Monitor > Routing Monitor**. Type OSPF for the **Type** and select **Apply Filter** to verify OSPF route.

Verify that traffic flows via the secondary tunnel.

From a PC1 set to IP:10.20.1.100 behind FortiGate 1, run a tracert to a PC2 set to IP:10.21.1.100 behind FortiGate 2 and vice versa. From PC1, you should see that the traffic goes through 10.2.1.2 which is the secondary tunnel interface IP set on FortiGate 2.

From PC2, you should see the traffic goes through 10.2.1.1 which is the secondary tunnel interface IP set on FortiGate 1.

Name	Type	Remote Gateway	Remote Port
To_FGT1_Primary	Static IP or Dynamic DNS	172.20.120.24	0
To_FGT1_Second	Static IP or Dynamic DNS	172.20.120.23	0

Name	Type	Remote Gateway	Remote Port
To_FGT2_Primary	Static IP or Dynamic DNS	172.20.120.123	0
To_FGT2_Second	Static IP or Dynamic DNS	172.20.120.127	0

IP Version	Type	Subtype	Network	Gateway	Interface
4	OSPF		10.21.1.0/24	10.2.1.2	To_FGT2_Second

IP Version	Type	Subtype	Network	Gateway	Interface
4	OSPF		10.20.1.0/24	10.2.1.1	To_FGT1_Second

```
C:\>tracert 10.21.1.100

Tracing route to TELBAR-PC [10.21.1.100]
over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms  10.20.1.1
  1  <1 ms    <1 ms    <1 ms  10.2.1.2
  2  1 ms     5 ms     <1 ms  TELBAR-PC [10.21.1.100]

Trace complete.
```

```
C:\>tracert 10.20.1.100

Tracing route to 10.20.1.100 over a maximum of 30 hops:
  0  <1 ms    <1 ms    <1 ms  10.21.1.1
  1  <1 ms    <1 ms    <1 ms  10.2.1.1
  2  1 ms     <1 ms    <1 ms  TAHER_THINK [10.20.1.100]

Trace complete.
```